Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WC Docket No. 16-106
Broadband and Other Telecommunications	)	
Services	)	

REPLY COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

William A. Check, Ph. D
Senior Vice President
Matthew Tooley
Vice President of Broadband Technology
Science & Technology

Christopher J. Harvie
Ari Z. Moskowitz
Mintz, Levin, Cohn, Ferris,
Glovsky & Popeo, P.C.
701 Pennsylvania Avenue, N.W.
Suite 900
Washington, D.C. 20004-2608

Rick Chessen
Loretta Polk
Jennifer K. McKee
National Cable & Telecommunications
Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431

July 6, 2016

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("NCTA") hereby submits its reply comments on the Notice of Proposed Rulemaking ("*Notice*" or "NPRM") in the above-captioned proceeding.[1/]

INTRODUCTION AND SUMMARY

The record in this proceeding reflects an extraordinary breadth and depth of opposition to the proposed rules. A diverse range of commenters, including academics, researchers, security specialists, start-up companies, online advertisers, civil rights organizations, large and small Internet service providers ("ISPs"), equipment makers, software providers, information technology ("IT") companies, edge entities, former government officials, and other Federal agencies all raise serious questions about the wisdom and efficacy of the core elements of the rules proposed in the *Notice*. While a handful of parties with no actual experience in operating networks or provisioning service to subscribers support the rules as proposed, the overwhelming consensus among the parties filing in this proceeding is that the Commission's proposal is unworkable, counterproductive, harmful to consumers and competition, and contrary to law.

1/ *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016).

The record in this proceeding is very clear: the Commission's proposal represents a radical departure from the proven and effective Federal Trade Commission ("FTC") framework that governed ISP privacy practices prior to reclassification. This is confirmed by submissions from FTC staff, current and former commissioners, and the overwhelming majority of commenters. FTC staff dubs the Commission's proposal "not optimal" and in conflict with the "different expectations and concerns that consumers have for sensitive and non-sensitive data."[2/] FTC staff raises over two-dozen concerns with the proposed rules, and recommends substantial alterations to the major components of the Commission's regime, including the scope of data covered by the rules, first-party marketing, opt-in/opt-out choice architecture, data security requirements, data breach obligations, and the method of soliciting choice.

Those concerns are amplified by others with experience in developing and administering the FTC framework. Former FTC Chairman Jon Leibowitz avers that the NPRM "does not identify any harms that necessitate rules that are different from the FTC framework" and that adoption of the proposed rules "would result in a detailed set of burdensome data privacy rules with no precedent in the FTC or other U.S. privacy regimes."[3/] Former FTC Commissioner Joshua Wright states that the Commission's rules "would inflict significant direct consumer welfare losses, observable in higher prices for broadband and other services offered by ISPs, result in indirect consumer losses including a greater rate of irrelevant advertising and more expensive content and services throughout the ecosystem, and chill innovation and experimentation in the ecosystem."[4/] Current FTC Commissioner Maureen Ohlhausen states that

---

2/ *See, e.g.,* Staff of the Bureau of Consumer Protection of the Federal Trade Commission ("FTC Staff") at 22.

3/ Comments of Jon Leibowitz ("Leibowitz") at 6.

4/ Joshua D. Wright, "An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy," (submitted by USTelecom in WC Docket No. 16-106) ("Wright") at 29.

"the FCC's approach is inconsistent with the FTC's long-standing framework" and "would hamper ISPs from competing with other businesses to serve consumers in data-driven industries, including online advertising."[5/] Neither the Commission nor supporters of the proposal, however, grapple with – let alone justify – the new costs and burdens inflicted upon consumers, competition, and innovation that will result from discarding the FTC Framework and subjecting ISPs to an unproven and manifestly cumbersome privacy regime.

Furthermore, numerous commenters confirm the validity of Professor Peter Swire's comprehensive assessment of ISP visibility over broadband customer data: ISPs do not have unique access to broadband customer data compared to other companies in the Internet ecosystem.[6/] The record simply cannot support a conclusion that ISPs should be subject to singularly onerous rules because they are somehow uniquely situated. To the contrary, the record demonstrates not only that ISP visibility over broadband customer data is rapidly shrinking, but also that ISPs have heightened incentives to effectively safeguard their customers' information and a track record of responsible conduct under the FTC framework. Survey information shows that consumers agree and believe by overwhelming margins that the same rules should govern all companies collecting broadband customer data, and that online information should be protected based upon the sensitivity of the data, and not the identity of the company collecting and using it.[7/]

[5/] Remarks of Maureen D. Ohlhausen, 2016 Advertising and Privacy Law Summit, *Reaction to the FCC's Proposed Privacy Regulation*, (June 8, 2016) ("Ohlhausen June 8 Speech") at 6.

[6/] Peter Swire, Justin Hemmings, Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, The Institute for Information Security & Privacy at Georgia Tech, at 23-24 (May 2016) (submitted in Docket No. WC 16-106) ("Swire Paper").

[7/] Progressive Policy Institute, Internet User Survey at 3.

The absence of any persuasive rationale for jettisoning the FTC's approach magnifies the legal infirmities of the Commission's proposed regime. Statutory analysis undertaken by a number of commenters demonstrates that the Commission's proposed rules cannot be grounded in Section 222 of the Communications Act or any of the other sources of authority invoked in the *Notice*, and there is nothing in the D.C. Circuit's recent decision in *United States Telecom Association v. Federal Communications Commission* that changes that analysis.[8/] Further, as thoroughly explained by constitutional law expert Laurence Tribe, adoption of the Commission's proposal also would violate the First Amendment.[9/] In addition, commenters oppose "harmonizing" the Commission's proposed regime with the privacy requirements of Section 631, and no persuasive rationale is offered for taking such an unwarranted and unlawful step.

The record shows that the Commission's departure from these basic tenets of regulatory parity and data sensitivity will confuse consumers and diminish their access to customized services, capabilities, and offerings – without offering any material improvement in privacy protection due to the ability of all other entities in the Internet ecosystem to use their data under a less stringent set of rules. Numerous commenters highlight the adverse effect on investment and innovation that will arise from inflexible constraints on broadband providers' ability to use data-driven insights to improve service and develop new products and capabilities.

As reflected in submissions from staff and former officials of the FTC and the vast majority of commenters, the policy defects of the FCC's proposal are legion:

- The huge swath of data covered by the proposal – which includes IP addresses, MAC IDs and other data elements that cannot on their own identify individuals – coupled

---

8/ *United States Telecom Ass'n v. FCC*, 2016 U.S. App. LEXIS 10716 (D.C. Cir. 2016).

9/ Laurence H. Tribe and Jonathan S. Massey, *The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment*, at 3-4 (May 27, 2016) ("Tribe").

with its stringent permissions regime threatens to encumber basic Internet functionality and burdens the provision of services and capabilities seamlessly enjoyed by broadband customers today. This is compounded by an unworkable "linkable" standard and unlawful treatment of de-identified data.

- The proposed restrictions on first-party marketing conflict with well-established policies supported by both the White House and the FTC, and would unduly interfere with the ability of consumers to benefit from new products and services offered by their broadband provider.
- The unwarranted departure from the FTC's core principle of establishing an opt-out/opt-in choice architecture that distinguishes between non-sensitive and sensitive uses of data harms consumers and competition.
- The narrowness of the specified exceptions to the permissions regime could adversely affect basic network operations, delivery via broadband transmission of services and capabilities requested by consumers, and efforts to protect ISP networks from cybersecurity threats, spam and malware.
- The unreasonable data security standard imposes a strict liability regime that unnecessarily encompasses a raft of non-sensitive data.
- The specifically enumerated data security requirements proposed by the Commission are out of step with well-established federal policy preferences for relying upon voluntary mechanisms and industry-driven solutions to secure networks effectively.
- The vastly overbroad data breach notification rules are predicated upon an ill-considered definition of "breach," and in conflict with virtually every existing breach notification law.

The record here should give the Commission pause, because it is rife with serious questions regarding the efficacy and utility of the proposed rules. Most commenters agree that embracing – rather than repudiating – the successful FTC Framework would be far more likely to safeguard privacy and benefit consumers, competition, and innovation than would the regime proposed in the NPRM. The Consensus Privacy Framework, developed by a broad cross-section of industry associations representing ISPs and technology companies, is closely aligned with the FTC's approach, as well as the Administration's core principles in the Consumer Privacy Bill of Rights. Its adoption would protect consumer privacy, apply similar standards to all online entities, minimize consumer confusion, and be less disruptive for the broadband ecosystem.

Importantly, it also will provide the flexibility the marketplace needs in order to innovate and evolve consumer online services.

I. THE COMMISSION LACKS THE LEGAL AUTHORITY TO ADOPT THE PROPOSED RULES

The record amply demonstrates that the Commission lacks the legal authority to adopt its proposed rules. First, commenters agree that Section 222 was intended to address only uses and disclosures of customer records generated and maintained in connection with the provision of voice telephony service.[10/] In enacting Section 222, "Congress directed the FCC to provide rules to safeguard telephone records – not to regulate privacy in the very different area of online data collection."[11/] Contemporaneously with the enactment of Section 222, Congress also amended the Communications Act to adopt provisions pertaining to consumer use of the Internet. If Congress intended Section 222 to apply to Internet usage data generated by consumers, "the text could have been drafted to include references to the Internet, as Congress did elsewhere in the Telecommunications Act of 1996."[12/] Indeed, Congress revisited the law in 2008 to bring "IP-enabled voice service" within the ambit of Section 222, an action deemed necessary because Congress viewed the provision as applying only to wireline and wireless *voice* service.[13/] Commenters likewise agree with NCTA that "the necessity of altering definitions to try to fit

---

10/ NCTA at 7-14; American Advertising Federation, *et al.* ("Advertising and E-Commerce Coalition") at 5-6; USTelecom at 28; Direct Marketing Association ("DMA") at 11-13; Verizon at 55; CTIA at 16-23; State Privacy and Security Coalition at 7.

11/ Advertising and E-Commerce Coalition at 5. Indeed, for nearly 20 years, the Commission viewed its authority under Section 222 as limited to regulation of uses and disclosures of telephone customer records. DMA at 5; Verizon at 56.

12/ DMA at 13; Advertising and E-Commerce Coalition at 5.

13/ *See* CTIA at 25; USTelecom at 29.

broadband privacy regulatory authority within Section 222 makes clear that the Commission is attempting to venture far beyond the authority granted to it by Congress."[14/]

Free Press incorrectly claims that the plain language of Section 222(c)(1) encompasses the regulations on ISP use of broadband customer data contemplated in the NPRM.[15/] As Comcast points out, merely "because the FCC has reclassified ISPs as telecommunications carriers does not magically expand Section 222's scope" beyond the telephony services it was designed to address.[16/] Indeed, in making its "plain language" argument, Free Press omits wording in the provision – "including the publishing of directories" – that reinforces Congress' intent to limit Section 222 to telephony, because the Commission itself views the publication of directories as relevant only to telephony service.[17/] Moreover, the statutory language quoted by Free Press underscores the incompatibility of Section 222 with the Commission's proposed rules. Section 222(c)(1) specifically references the term "customer proprietary network information ("CPNI"), defined as information that is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[18/] As USTelecom points out, broadband customer "information is NOT available ONLY to the BIAS provider by the customer *solely by virtue of the carrier-customer relationship*. In the context of BIAS this entire concept is a fallacy."[19/] As

---

14/ DMA at 13; *see also* Comcast at 66-68; NCTA at 11.

15/ Free Press at 8.

16/ Comcast at 67-68 *citing American Bankers Ass'n v. SEC*, 804 F.2d 739, 754-55 (D.C. Cir. 1986) (agency cannot "change basic decisions made by Congress" or "use its definitional authority to expand its own jurisdiction").

17/ *See* NPRM at ¶ 64.

18/ 47 U.S.C. § 222(h)(1).

19/ USTelecom at 7 (emphasis in original); *see also* AT&T at 2 ("The commercial entities with access to CPNI were generally all telecommunications carriers subject to Section 222, and there were no unregulated companies collecting and trading the same information for marketing purposes. In contrast, the Internet owes its explosive growth to the free flow of customer-specific information within a sprawling ecosystem of online companies."); *id.* at 100-03.

the record in this proceeding amply demonstrates, the broadband customer data that the Commission's proposal would cover is broadly available to a wide variety of entities in the Internet ecosystem.[20/]

Second, Section 222(a) is not a standalone grant of authority to regulate personally identifiable information ("PII").[21/] The text, history, and structure of Section 222 preclude reading a separate mandate to protect PII into Section 222(a).[22/] As the Direct Marketing Association notes, "the Commission's construction of Section 222 misreads the purpose of subsection (a), which was to make clear that the duties imposed by the statute are to apply to all providers of telephony-related telecommunications services—not only to a handful of carriers, as was the case in the original Senate bill."[23/]

The Center for Democracy and Technology ("CDT") strains to argue that the legislative history of the 1996 Act supports the view that Congress intended to include PII within the scope of Section 222.[24/] CDT, however, ignores the fact that other provisions of the Communications Act unequivocally show that Congress knows how to make explicit its intention to impose constraints on the use of PII when it wishes to do so – but it did not do so in Section 222.[25/] Nor could it have intended to do so, based upon its decision to specifically define subscriber name, address and telephone number information as publicly available "subscriber list information" for

---

20/ *See, e.g.,* AT&T at 10-12; Comcast at 30-33; Verizon at 22; Comments of Richard Bennett ("Bennett") at 6; Professor Christopher Yoo, Center for Technology Innovation and Competition ("Yoo") at 4; International Center for Law & Economics ("ICLE") at 9-10, Appendix A.

21/ NCTA at 14-18.

22/ Electronic Transactions Association at 9-10; DMA at 13; Verizon at 57; Competitive Carriers Association at 12; AT&T at 106; USTelecom at 29-30.

23/ DMA at 13.

24/ Center for Democracy and Technology ("CDT") at 10-11.

25/ *See, e.g.,* 47 U.S.C. §§ 338, 631; *see also* CTA at 6; Mobile Future at 10-11.

purposes of Section 222,[26/] a Congressional determination that CDT and other supporters of the Commission's rules likewise fail to grapple with. In fact, Congress chose to use entirely different terminology in Section 222(a), targeting "proprietary" information rather than "personally identifiable information," which militates against conflating the two terms.[27/]

Further, the structure and text of Section 222 is at odds with the Commission's proposed interpretation of Section 222(a). As CTIA writes, it is "coherent and internally consistent only if 'proprietary information' [in 222(a)]… is interpreted to be coterminous with CPNI."[28/] NCTA and several commenters showed that Congress's decision to not include subsection (a) in the list of provisions that subsections (e) and (g) supersede – and to exclude the phrase "customer proprietary information" from the preamble to the list of exceptions in subsection (d) – indicates that Congress did not view subsection (a) as providing protection for a data set beyond CPNI.[29/]

Public Knowledge erroneously claims that a portion of a footnote to the introductory paragraph of a 2007 order constitutes a prior Commission "holding" that "personally identifiable information" is included within the definition of CPNI.[30/] Public Knowledge never explains why the Commission would hide the "central holding" and "central basis" of that 2007 Order in a stray phrase in a single footnote. Nor does Public Knowledge explain why the Commission would use a footnote to *sub silentio* overrule its express determination in 1998 that the core components of anyone's notion of PII – subscriber name, address, and telephone information –

26/ *See* NCTA at 14-15; Internet Commerce Coalition at 13-14; State Privacy and Security Coalition at 6-7; Direct Marketing Association at 13-14.

27/ *See* Verizon at 59; CTA 5-7; Mobile Future at 11-12.

28/ CTIA at 25.

29/ NCTA at 16-18; CTIA at 27-28; Verizon at 57; AT&T at 106; Electronic Transactions Association at 11.

30/ Public Knowledge at 27 *citing Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, 22 FCC Rcd 6927, at n. 2 (2007).

are not CPNI and expressly excluded from the definition of that term,[31/] and to supersede the Congressional determination that such information is actually "subscriber list information."[32/]

Third, commenters agree that the Commission misapplies the statutory directive that use and disclosure constraints on information protected by Section 222 be applied only to "individually identifiable" information covered by that provision.[33/] While the statute clearly specifies that CPNI which is not "individually identifiable" is exempt from the restrictions of Section 222, the Commission proposes to unlawfully rewrite that carve-out by limiting its applicability only to CPNI that is both not individually identifiable *and* aggregated.[34/] Parties that favor subjecting de-identified, non-aggregated data to the permissions regime proffer no plausible reading of the statute to support that position.[35/] Under the statute, CPNI either identifies an individual or it does not. So long as it does not – due to the absence or removal of individual identifiers – it is not covered by the restrictions of Section 222, irrespective of whether it is aggregated.[36/]

As NCTA noted in its initial comments, adherence to the statutory directive to constrain only uses or disclosures of "individually identifiable" CPNI is critical because the breadth of data proposed to be covered by the rules encompasses numerous data elements that – on their own –

31/ NCTA at 14; *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Information and Other Customer Information*, Order, 13 FCC Rcd 12390, ¶¶ 8-9 (1998).

32/ Unsurprisingly, that Order lacks any express articulation or delineation of the new data elements that were putatively deemed to be CPNI as a result of the footnote.

33/ T-Mobile at 34-35; Sprint at 7; Verizon at 58.

34/ NPRM at ¶ 165.

35/ *See* Electronic Frontier Foundation ("EFF") at 16.

36/ T-Mobile at 34-35; IMS Health at 7; AT&T at 68.

cannot identify an individual.[37/] Commenters concur that data elements like IP addresses and MAC IDs should not be deemed CPNI subject to the use and disclosure restrictions of Section 222 either because these elements cannot on their own identify individuals or because they fall outside the definitional limits of CPNI.[38/]

Fourth, numerous commenters maintain that the proposed rules cannot pass muster under the First Amendment.[39/] Professor Laurence Tribe states that the Commission's proposal "runs afoul of fundamental First Amendment limits on the FCC's authority to regulate customer information" and that the proposed rules are "even *more constitutionally problematic* than the CPNI regulations invalidated by the Tenth Circuit."[40/] Notwithstanding claims to the contrary,[41/] Professor Tribe's submission demonstrates that the proposed rules cannot meet the *Central Hudson* test for intermediate scrutiny:[42/]

37/ NCTA at 23-24; Internet Commerce Coalition at 13-14 (The Commission's proposal "sweeps into the statute information that travels widely across the Internet whenever a user communicates. . . . Because this information is widely available by virtue of the ordinary operation of the Internet, there should be no restrictive requirements on any entity that holds it.").

38/ *See, e.g.,* NCTA at 21-23; Comcast at 77-81; CTIA at 44; Audience Partners at 9-13; Farsight Security at 6 ("IP addresses *are assigned by the provider to the customer, whether via DHCP or as a static IP*. As such, the data flows the 'wrong way' (from the provider to the customer rather than vice versa) to be considered CPNI.") (emphasis in original); Bennett at 3 ("CPNI would not include customer location or the IP addresses of the customer's Internet destinations because such information is known by parties other than the telecommunication provider and the customer.").

39/ *See,* e.g., NCTA at 32-33; CTIA at 72-92, USTelecom at 31-32, AT&T at 91-99, Comcast at 89-99.

40/ Tribe at 3-4.

41/ *See* Public Knowledge at 37-39.

42/ *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 566 (1980) (constitutionality of commercial speech restrictions assessed by examining (1) "whether the asserted governmental interest is substantial," (2) "whether the regulation directly advances the governmental interest asserted," and (3) "whether it is not more extensive than is necessary to serve that interest.").

- The burden on speech from the Commission's proposal is substantial in light of the "sweeping opt-in consent requirements" and their imposition on only a small segment of the market;[43/]

- The Commission has asserted no substantial government interest for regulating ISPs more strictly than other actors with the same information, or for regulating the use, as opposed to the disclosure, of information already in the possession of ISPs;[44/]

- The proposed rules do not advance the asserted government interest given the different treatment of similarly situated edge providers with respect to user data and their restrictions on uses of data that do not even implicate sharing with third parties;[45/] and

- The proposal is more extensive than necessary to serve the government's interest given the successful history of the FTC Framework.[46/]

While Public Knowledge suggests that the Commission can satisfy *Central Hudson* so long as it "clearly articulates its reasoning,"[47/] Professor Tribe notes that the "FTC regulatory regime provides an obvious alternative that is less speech-suppressing and demonstrates that the FCC's proposal fails the third prong of *Central Hudson*.[48/] Further, as Professor Tribe also points out, the Commission's proposed rules may be held to an even more stringent standard than the intermediate scrutiny of *Central Hudson*.[49/] In *Sorrell v. IMS Health, Inc.*, the Supreme

---

43/ Tribe at 16.

44/ Tribe at 18-21.

45/ Tribe at 22-29. Apart from its infirmities under the *Central Hudson* test, the proposal also implicates additional constitutional concerns because it forges content-based distinctions with respect to restrictions on marketing communications-related services versus marketing non-communications-related services. Tribe at 30-31.

46/ Tribe at 33-38.

47/ Public Knowledge at 37-39.

48/ Tribe at 6. Professor Tribe also explains that the D.C. Circuit's decision in *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) cannot sustain the rules proposed here. While that decision focused on the imposition of a "limited opt-in consent requirements" aimed at restricting the sale of customer information to data brokers, the instant proposal imposes a default opt-in regime applied to an ISP's own use of broadband customer data and implicates tailoring flaws and content-based distinctions that were not present in *NCTA v. FCC*. Tribe at 7.

49/ Tribe at 13-14; *see also* NCTA at 32, n.105.

Court held that the First Amendment protects not only the right to speak, but also the right to gather and process information in preparation for speech.[50/] As Professor Tribe writes, the Court "left open the possibility that restrictions like those proposed by the FCC here should receive stricter First Amendment protection than the *Central Hudson* test," because "analysis of customer information that serves as a foundation for expressive activities is a valuable form of fully protected First Amendment speech – not merely commercial speech."[51/]

Fifth, commenters agree with NCTA that the other sources of authority cited in the *Notice* cannot support the proposed rules. Section 201(b) is not available because the specific requirements (and limitations) of Section 222 supersede the general provisions of Section 201.[52/] Any contrary "view of the Commission's authority would render much of the rest of Title II, with its minutely detailed statutory provisions and related rules, exceptions and exemptions, largely if not completely superfluous."[53/] Section 201(b) also limits the Commission's authority to regulate to where it is "necessary . . . to carry out the provisions of [the Act]."[54/] As Verizon points out, however, a proposal that reduces choice, such as the proposed ban on data-related discounts, "cannot be said to carry out Section 222, because it contradicts Section 222's emphasis on customer choice and consent."[55/]

50/ *Sorrell v. IMS Health, Inc.,* 564 U.S. 552, 570 (2011).

51/ Tribe at 13-14, *citing Sorrell*, 564 U.S. at 567, 571; *Retail Digital Network, LLC v. Appelsmith*, 810 F.3d 638, 648 (9th Cir. 2016) (holding that *Sorrell* modified the *Central Hudson* test to require courts to apply heightened scrutiny when a "law burdening non-misleading commercial speech about legal goods or services is content- or speaker-based.").

52/ NCTA at 25; *see also* CTIA at 60-63; AT&T at 108-109; USTelecom at 31-32.

53/ ACA at 17.

54/ 47 U.S.C. § 201(b).

55/ Verizon at 48.

Section 705 fails as a source of authority because activities permitted by the Wiretap Act cannot be proscribed by Section 705.[56/] T-Mobile correctly notes that "Section 705 addresses issues surrounding piracy and the unlawful interception of content… It cannot provide authority for the dramatically expansive privacy rules proposed in the NPRM, which concern issues other than the content of the communications at issue"[57/] While EFF claims that Section 705 does in fact provide an independent source of authority,[58/] its comments appear not to have considered the multiple ways in which the application of Wiretap Act provisions and jurisprudence would severely hamstring – if not completely defeat – operation of the rules proposed by the Commission.[59/]

Section 706 only grants authority to an extent not inconsistent with the Communications Act, and the proposed rules are, as shown, inconsistent with Section 222 in several respects.[60/] Further, Section 706 does not empower the Commission to regulate ISPs in any way that fails to encourage broadband deployment or remove barriers to investment, but the "unprecedented level of regulation of ISPs' proprietary information and advertising will discourage investment in and deployment of broadband."[61/] As WISPA notes, the Commission itself barely attempts to articulate how the proposal will encourage deployment, claiming only that the proposed requirements "have the *potential* to increase customer confidence in BIAS providers' practices,"

56/ NCTA at 26-29; *see also* Verizon at 62 ("Section 705 is thus an anti-wiretapping statute… and is not a general privacy provision."); CTIA at 63-64; AT&T at 110.

57/ T-Mobile at 22.

58/ EFF at 2-3.

59/ *See* NCTA at 26-29.

60/ NCTA at 29; *see also* CTIA at 65-71 (The proposed rules are also contrary to Section 706's broadband deployment purpose as they will inhibit investment in broadband.); AT&T at 110-112 (Any authority derived via Section 706 on the basis of privacy concerns chilling broadband adoption would apply even more so to edge provider data collection and use.).

61/ Washington Legal Foundation at 8.

without providing any economic or market studies to support this "potential" outcome.[62/] Indeed, the evidence indicates that the proposal will in fact negatively impact deployment.[63/]

Free Press agrees that "reliance on Section 706 poses serious issues," characterizing the Commission's suggestion to use Section 706 as "awkwardly cast[ing] privacy protections and rights as a mere broadband deployment spur."[64/] Free Press adds that while "[s]o-called edge providers unquestionably can and do threaten the privacy of their users" Section 706 could, but should not, be "stretch[ed]" to encompass edge providers.[65/]

Sixth, the Commission cannot and should not harmonize the proposed rules with Section 631. As NCTA and others explain, provisions of the Cable Act itself statutorily restrict the Commission from grafting any portion of the rules proposed in this proceeding onto the privacy provisions of Section 631.[66/] Notwithstanding EPIC's suggestion that the Commission apply the proposed linkability standard "to all of the statutes and regulations within its jurisdiction,"[67/] it cannot do so with regard to Section 631, since PII is defined in the statute and has been interpreted by the courts.[68/] Further, the Commission itself has stated that Section 631is enforced by the courts and not the Commission.[69/] Nor would there be any policy benefits to "harmonizing" the proposed rules with the requirements of Section 631. The Cable Act's privacy provisions have successfully protected cable subscriber PII for over thirty years, and it

---

62/ WISPA at 7.

63/ *Id*. at 7-8; T-Mobile at 23; NCTA at 29.

64/ Free Press at 17-18.

65/ *Id*. at 18.

66/ *See, e.g.,* NCTA at 35-36; ACA at 18-19; Comcast at 108-109.

67/ EPIC at 19.

68/ *See* Comcast at 110, n.317; NCTA at 22, n. 64.

69/ *See*, NCTA at 36; ACA at 19.

makes no sense to discard an effective and proven set of obligations in favor of an untested regime widely considered to be overbroad and excessively cumbersome. As Comcast notes, "any suggestion that the privacy rules applicable to cable services should be changed is a solution in search of a problem and should be abandoned."[70/]

Seventh, the proposed data security and data breach rules are contrary to law and longstanding federal policy.[71/] The State Privacy and Security Coalition states that the "proposed information security and breach notice requirements are totally unprecedented in the United States and go far, far beyond state information security and breach notice requirements."[72/] As explained in NCTA's initial comments, when Congress intends to impose specific and granular data security requirements, it does so expressly. Nothing in Section 222 signals any Congressional intent to authorize the Commission to adopt the specific, prescriptive data security regulations proposed in the *Notice*.[73/]

The proposal also conflicts with well-established Federal policy that relies upon voluntary mechanisms and "explicitly calls for *companies* to conduct their own risk assessments and then develop individualized cybersecurity programs to address identified risks."[74/] But the *Notice* would "effectively take that decision-making away from companies and insert the Commission… even though the FCC has no particular expertise in that area."[75/] And as discussed below, commenters highlight the numerous ways in which the FCC's data security and

---

70/ Comcast at 110.

71/ *See* NCTA at 33-35.

72/ State Privacy and Security Coalition at 11.

73/ *See* NCTA at 34.

74/ AT&T at 79-80 (emphasis in original); CTIA at 156-158; NCTA at 34.

75/ AT&T at 80.

breach rules would in fact harm, rather than improve security.[76/] Given the unprecedented nature of the Commission's data security proposals, and the extent to which they depart from established frameworks, the Administrative Procedure Act (APA) requires that the Commission provide "a satisfactory explanation for its action" that justifies the new rule based on the facts.[77/] Yet, as commenters point out, "[t]he *Notice* fails to adequately justify the purported benefits of such a prescriptive regulatory approach against [its] inevitable costs,"[78/] and thereby contravenes the APA prohibition against arbitrary and capricious decision-making."[79/]

II. THE FCC'S PROPOSED RULES DEPART FROM THE FTC FRAMEWORK IN WAYS THAT WILL HARM CONSUMERS AND THWART COMPETITION AND INNOVATION

A. The Comments Underscore the Material Differences Between the FCC's Proposal and the FTC and White House Privacy Frameworks

In what commenters agree is "a radical break from… two decades of consensus,"[80/] the Commission proposes an overly restrictive and prescriptive set of rules without ever asking "the question of whether the current system – developed based on the Federal Trade Commission's broad policy requirements – actually needs to be replaced."[81/] Many commenters, including FTC staff itself, recount the manifold ways in which the Commission's proposed rules differ from the longstanding FTC Framework.[82/] Among the differences highlighted by the FTC staff:

76/ *See infra* Sections III.C-D.

77/ *Motor Vehicle Mfrs. Ass'n v. State Farm Mutual Auto Insurance Company*, 463 U.S. 29, 43 (1983).

78/ CTA at 10; *see also* CenturyLink at 39 ("Without substantial changes, many of these further requirements would impose tremendous costs with limited benefit.").

79/ AT&T at 79.

80/ AT&T at 37.

81/ ADTRAN at 3.

82/ *See, e.g.,* FTC Staff at 7-36; Leibowitz at 6-12; Internet Commerce Coalition 19-20; Comments of FTC Commissioner Maureen Ohlhausen ("Ohlhausen") at 1-2; CTA at 11-13; IMS Health at 14-15.

- *Technological/Competitive Neutrality*. FTC staff questions the utility of subjecting ISPs to a different set of privacy and security rules than other entities that "collect and use significant amounts of consumer data."[83/]

- *Scope of Covered Data*. The FCC proposes an overbroad and unqualified linkability standard that could encompass "almost any piece of data"[84/] in place of the FTC's "reasonably linkable" standard.

- *First Party Marketing*. Unlike the FTC Framework's recognition of implied consent for most first party uses of data, the FCC proposal adopts a narrow conception of implied consent that contravenes consumer expectations.[85/]

- *Opt-in/Opt-out Choice*. The FTC supports opt-in consent only for collection and use of sensitive data and a default opt-out for all other, non-sensitive data, while the FCC proposes to make opt-in the default for nearly all data uses regardless of sensitivity.[86/]

- *De-identification*. FTC staff comments cite guidance from prior reports exempting de-identified data from choice obligations irrespective of whether or not it is aggregated,[87/] while the FCC proposes to exempt only data that is both de-identified and aggregated.

- *Data Security*. The FTC directs companies to employ reasonable data security practices, while the FCC imposes a strict liability security standard and a specific set of mandated data security measures.[88/]

- *Data Breach Notification*. The FCC subjects a large swath of data – both sensitive and non-sensitive – to a short breach notification timetable of 7-10 days. The FTC suggests a notice timetable of 30-60 days that would be applied to a narrower set of customer data.[89/]

While the FTC diplomatically characterizes the regulatory asymmetry effectuated by the FCC's proposal as "not optimal,"[90/] other commenters are more straightforward. Citing the lack

---

83/ FTC Staff at 8.

84/ *Id.* at 9.

85/ *Id.* at 22-23.

86/ *Id.* at 22-23, 35.

87/ *See id.* at n.67.

88/ *Id.* at 27.

89/ *Id.* at 31-33.

90/ *Id.* at 8; *see also* Ohlhausen June 8 Speech at 6.

of any evidence that the FTC's regime is inadequate,[91/] commenters call the FCC's proposal "as irrational as it is irreconcilable with two decades of consensus federal policy,"[92/] "completely unnecessary and counterproductive,"[93/] and in "direct contradict[ion to] the privacy framework that the Commission cites as the basis for its proposal."[94/] The FCC's proposal is also a "significant departure" from the White House's technology neutral approach to privacy and cybersecurity,[95/] and more stringent even than the overzealous European privacy regulation[96/] As former FTC Chairman Jon Leibowitz observes: "The Privacy NPRM, if adopted as proposed, would result in a detailed set of burdensome data-privacy rules with no precedent in the FTC or other U.S. privacy regimes, and is inconsistent with the privacy obligations applied to the rest of the economy. Moreover, the NPRM does not identify any harms that necessitate rules that are different from the FTC framework."[97/]

Privacy advocates belie their hostility to the FTC Framework by enthusiastically embracing the Commission's repudiation of several of its key features – and, in some cases, encouraging it to go farther.[98/] But their aversion to the FTC's model provides no empirical grounding for the Commission's decision to jettison core elements of that framework.

91/ *See, e.g.*, ADTRAN at 3; Comments of Professor J. Howard Beales ("Beales") at 2; ITI at 8; Consumers' Research at 11-12; Wright at 6-7.

92/ AT&T at 38.

93/ ANA at 5.

94/ DMA at 3.

95/ Internet Commerce Coalition at 6-7.

96/ Internet Commerce Coalition at 4.

97/ Leibowitz at 6.

98/ *See, e.g.,* EFF at 8 (arguing the Commission should eliminate the category of "implied approval"); Public Knowledge at 28-31 (rejecting implied opt-out consent for first-party marketing of all related services); EPIC at 6-10 (repudiating the notice and choice model and advocating for default opt-in for all data collection and use).

Nor does the FCC offer evidence of the failure of the FTC's regime.[99/] The *Notice* "identifies no adverse consequences to consumers that have resulted from broadband provider privacy practices under the FTC Framework."[100/] Instead, the Commission's proposed rules inflict severe constraints – relative to the FTC Framework – on the ability of ISPs to use data-driven insights to provide new products, improve service, and enhance the customer experience without ever explicating how such a drastic change from the pre-reclassification *status quo* benefits consumers, competition, and innovation.[101/] Not only does the proposal withdraw from consumers the benefits associated with applying the FTC Framework to ISPs, it does so without providing any material benefit to privacy. As former FTC Commissioner Wright observes:

> [C]onsumers' privacy interests are not better served under the NPRM than they are today. Consumers can – and those who care, already *do* – make informed decisions about whether to permit certain marketing uses of their data today. Thus, the only purported value of the NPRM, i.e., enhancing privacy, is essentially nonexistent as a practical matter.[102/]

The FTC Framework is "a superior model to support innovation" that balances the objective of safeguarding broadband customer privacy while still affording ISPs the necessary flexibility to provide their customers with the benefits of data-driven insights, capabilities and services.[103/] The Commission's decision to abandon that model is unwise and unwarranted.

99/ Beales at 2; ANA at 16 ("The NPRM offers little explanation or justification regarding how this significant departure from the FTC's privacy framework will benefit the public.").

100/ Beales at 2; Leibowitz at 6.

101/ Some commenters express concern that the imposition of such constraints is itself an underlying objective of the proposal. *See* ITIF at 6 ("More troubling than the FCC overlooking these issues is the possibility that the proposed rules stem from a desire to lock BIAS providers out of data-driven business model innovation, consigning them to mere transport providers."); USTelecom at 11 (noting the "Commission's seeming hostility to the benefits of using information to benefit consumers").

102/ Wright at 28.

103/ ITIF at 10.

B. The Record Demonstrates That the Commission Cannot Justify the Imposition of More Stringent Privacy Rules on ISPs

The comments resoundingly demonstrate that there is no justification for imposing more stringent privacy rules on ISPs. The notion that ISPs have greater visibility over customer data "is factually wrong, outdated, and drives a proposed privacy regime that fails to take a comprehensive and uniform approach to protect consumers' privacy throughout the entire Internet ecosystem."[104/] Numerous parties note that large edge providers have access to the same, if not more, broadband customer data, and that ISPs have heightened incentives to effectively safeguard their customers' data and a track record of responsible conduct under the FTC framework.[105/]

As Verizon explains, consumer use of "multiple broadband providers and the increasing prevalence of encryption mean that broadband providers have little more (and often much less) access to consumer data than other Internet companies."[106/] ISP visibility of broadband customer data is less comprehensive than that of large edge providers and is shrinking rapidly. This fundamental insight, explored at length by Professor Peter Swire, is supported by many

---

104/ CWA at 3; *see also* T-Mobile at 5 ("According to the Commission, BIAS providers 'have the ability to capture a breadth of data that an individual streaming video provider, search engine or even e-commerce site simply does not.' This underlying premise is false."); Leibowitz at 7 (noting that "the precipitous rise of encryption and proliferation of networks and devices have limited the scope of customer data available to broadband providers, while other companies operating online have gained broader access to consumer data across multiple contexts and platforms"); Comcast at 26-30.

105/ NCTA at 46-53; Internet Commerce Coalition at 9-10; AT&T at 26-29; ITIF at 3-4; USTelecom at 3-5; Comcast at 27-33; Advanced Communications Law and Policy Institute at 2; Electronic Transactions Association at 6-7.

106/ Verizon at 4; Comcast at 27 ("[A]ny one ISP is the conduit for only a fraction of a typical user's online activity. This is because consumers increasingly use a number of different devices across multiple ISPs for Internet access.").

comments emphasizing that "the breadth of data collected from a wide range of sources is substantial, and substantially greater than for ISPs."[107/]

As encryption use rises and the plethora of tools available for consumers to mask data expands, "the trend is clear and strong in the direction of a reduction in BIAS access to consumer data."[108/] Network engineer Richard Bennett explains that in an unencrypted scenario, "there is no meaningful difference between the information visible to ISPs and to web services."[109/] When data is encrypted, however, "there is an enormous difference between the small pool of information available to ISPs and the much larger pool visible to web services."[110/]

And it is not just encryption that limits visibility to ISPs. While incorrectly asserting that ISPs "arguably come closest to having a total view of U.S. internet users," CDT also notes that "most adults stay connected when they leave home through smartphones."[111/] But this is evidence that no single ISP can have a total view of any individual subscriber's Internet use – people connect through multiple different ISPs each day at home, over mobile networks, at work,

---

107/ ICLE at 9, Appendix A (detailing the information collection practices of non-ISPs); *see also* American Commitment at 2 ("The Commission asserts that ISPs are uniquely situated to collect user information, but the best available data shows a very different picture."); ACLP at 14 ("ISPs appear likely to explore online advertising as a way to generate new revenues, but even then their market share and ability to gather data on a large scale – i.e., across multiple networks, devices, services, and location – will be limited and greatly overshadowed by the efforts of incumbent companies like Facebook."); ITIF at 5 (ISP data visibility "is far less complete than advocates describe… And most of these customers use the same browser, search engines, social media platforms, and e-commerce sites across devices and service providers."); Yoo at 4 ("[U]sers are making broader use of HTTPS and other forms of security in both browsers and in mobile apps. Although ISPs would continue to be able to observe the locations to and the patterns with which traffic flows, they will not be able to observe any of the content. Edge providers, in contrast, have ready access to the complete content of all of the data regardless of the level of encryption."); Comcast at 30 ("Importantly, non-ISPs have access to the *same information* to which ISPs have access, and, as Professor Swire found, *often much more*.") (emphasis in original).

108/ ITIF at 4; *see also* AT&T at 44; Comcast at 28 ("ISPs' visibility into the Internet behavior of their customers is also limited because more and more of the traffic that they do carry is encrypted by a third party… The percentage of Internet traffic that is encrypted is relatively high and rising rapidly).

109/ Bennett at 5.

110/ Bennett at 5.

111/ CDT at 18.

and in coffee shops.[112/] Compared to edge providers that collect data from broadband users across numerous devices and locations, there is nothing unique or uniquely concerning about ISP access to consumer data.[113/] For example, Facebook recently announced that it is using cookies and other embedded code on third party websites to track individuals for targeted advertising, regardless of whether the visitor is even a Facebook user.[114/]

Public Knowledge's attempts to cast doubt on Professor Swire's findings regarding ISP visibility are unavailing.[115/] For example, Public Knowledge downplays encryption and claims that Swire fails to consider "predictive marketing," which emphasizes access to Internet metadata, rather than to the content of broadband transmissions.[116/] Upturn likewise contends that "over a longer period of time, metadata can paint a revealing picture about a subscriber's habits and interests.[117/] However, Swire never contends that encryption can mask ISP access to metadata about Internet usage by their customers[118/] – he simply makes clear that ISPs are not

---

112/ *See* NCTA at 47.

113/ Bennett at 6 ("And unlike ISP-visible objects, web cookies function across platforms and devices. Users of a particular browser, such as Chrome, access the same cookies across desktops, laptops, tablets, and smartphones, whether connected by wired residential ISPs, business ISPs, or mobile ISPs."); Comcast at 29 ("In contrast to ISPs' limited ability to access consumer's web traffic, many non-ISP content and service providers are able to collect significant amounts of information due to the numerous ways in which they interact with and track consumers across devices and Internet connections. These other types of entities have access to an enormous amount of consumer information.").

114/ Amar Toor, *Facebook Begins Tracking Non-Users Around The Internet*, THE VERGE (May 27, 2016), http://www.theverge.com/2016/5/27/11795248/facebook-ad-network-non-users-cookies-plug-ins.

115/ Public Knowledge at 6-23.

116/ *Id.* at 6-11; *see also* New America's Open Technology Institute at 4.

117/ Upturn at 7.

118/ It is worth noting, however, that the IETF is working on adding encryption support for additional Internet control protocols, such as domain name system and time. NCTA at 48, n.174.

unique in this respect as the same or similar data is often available to others and that ISP access to such data is less comprehensive than perceived.[119/]

Public Knowledge and Upturn also suggest that Swire overestimated the amount of traffic that is encrypted.[120/] But neither disputes Swire's data that encryption is increasing or that it diminishes the scope of data visible to ISPs. Upturn also argues that encryption is not 100% effective as various "side channel methods" have allowed researchers to identify search queries and websites visited without decrypting encrypted traffic.[121/] But the theoretical ability of trained experts with sophisticated tools and massive computing power employing what Upturn understates as "some amount of effort" to potentially decipher snippets of encrypted traffic does not offer grounds for disregarding the significance and impact of encryption on ISP visibility over customer data.[122/] Further, Upturn's suggestion that VPNs are used less frequently in the United States than they are in other countries – where they are employed to circumvent online censorship and gain access to restricted content – simply underscores the potential efficacy of VPNs for those who wish to employ them, particularly in countries with more restrictive online regulatory frameworks.

119/ *See, e.g.,* Swire Paper at 35, 123; Richard Bennett, *Privacy and the Internet: What the FCC Doesn't Get*, HighTech Forum (May 17, 2016), http://hightechforum.org/privacy-internet-fcc-doesnt-get/ ("[T]he best place to be in the Internet to track users is in the browser. . . . The browser knows if I read the pages I visit because it sees me scrolling and tracks my mouse clicks. It knows when I forward links to the pages I read to others. And it knows which paragraphs I re-read."); AT&T at 27 ("In contrast to ISPs, edge providers like Google and Facebook can track users across devices and networks because users routinely log into the same accounts on different devices and across different ISP networks. Just as important, even Internet companies that (unlike Google) cannot directly track customers across the Internet can still acquire comprehensive information about those same customers from third-party data brokers."); Verizon at 22 (noting that "the browser or operating system running on [a mobile] device can obtain the same information about each of the visits to each of the websites" and "have access to virtually all information regarding the activities of customers while using their devices. And there are advertising networks that use cookies on multiple sites to track customers moving from one website to another").

120/ Public Knowledge at 19-20; Upturn at 3-6.

121/ Upturn at 7-9.

122/ Upturn at 8.

Public Knowledge also expresses concern that cable ISPs have access to both online activity and set top box data that could be combined together,[123/] without articulating any specific harms arising from this circumstance. The use of set top box data is already subject to a robust and comprehensive privacy regime under Section 631 and, notwithstanding the fact that the ability to combine such data has existed for years, there have been no judicial or FTC enforcement actions proscribing such conduct.[124/] Further, there is nothing unique about cable providers having access to both Internet activity and video viewing data relative to several other large edge providers, save for cable providers being uniquely covered under long-standing and robust privacy rules governing viewing data. And ISPs are also not unique in their ability to combine online and offline data. As AT&T describes, edge providers – both those that can track users across devices and networks, such as Google and Facebook, and those that cannot – have the ability to obtain from data brokers comprehensive profiles of consumers that combine online and offline data.[125/]

Public Knowledge selectively quotes Professor Feamster as claiming that the Swire paper includes "technical inaccuracies" that "reflect some basic misunderstandings of Internet protocols." In fact, after a series of exchanges between the two academics, Professor Feamster concluded that upon "more careful review of the paper, I have not found anything in the report that I believe is incorrect."[126/] Further, in contrast to Public Knowledge, Professor Feamster

---

123/ Public Knowledge at 8.

124/ *See* FTC Staff 4-5.

125/ AT&T at 27; *see also* Kashmir Hill, *Facebook is Now Keeping Track of the Stores You Go To IRL*, FUSION, June 16, 2016, http://fusion.net/story/315575/facebook-smartphone-location-tracking/.

126/ Peter Swire, *Addendum: Online Privacy and ISPs*, The Institute for Information Security & Privacy at Georgia Tech, 3 (Mar. 6, 2016), *available at* http://www.iisp.gatech.edu/sites/default/files/documents/addendum_03-06-16_isp_access_to_data_working_paper_.pdf.

acknowledges the potential harms arising from the breadth and the rigidity of the Commission's proposed rules, noting that excessively stringent restrictions on broadband customer data collected and used by ISPs "will harm the security and performance of the Internet and threatens to inhibit research innovation."[127/] He concludes that "ISPs should certainly take measures to protect data that could pose risks to user privacy, but those measures should be commensurate with the risks that the data poses to consumers."[128/] This aligns with the conclusions of numerous commenters that the Commission's proposed rules should be calibrated to the sensitivity of the data being used or disclosed.[129/]

Not only do ISPs lack any advantages relative to large edge providers with regard to visibility of broadband customer data, they also have heightened incentives to safeguard customer data.[130/] The Commission's own orders acknowledge that the "continuing relationship" ISPs have with their customers reduces the risks of misuse of customer data compared to other entities that may have more ephemeral – and less direct - interactions with broadband consumers.[131/] The record confirms the validity of that assumption.[132/] Thus, any "claim that legally binding principles are the only safeguards against 'commercial motivation' to

---

127/ Comments of Professor Nick Feamster ("Feamster") at 4,7.

128/ Feamster at 8.

129/ *See, e.g.,* NCTA at 6; FTC Staff at 20, 22-23.

130/ NCTA at 51-52.

131/ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, at ¶¶ 37, 55 (2002).

132/ T-Mobile at 9-10; Comcast at 38-39; CenturyLink at 28 ("BIAS providers' primary incentive is to attract and retain customers. We could not do so if we exploited our customers or otherwise failed to meet customer expectations, such as by using and disclosing customer information in ways contrary to our customers' expectations and desires.").

mistreat consumers is flatly wrong. ISPs have every incentive to earn and keep the trust of their customers without regulation."[133/]

Likewise, the competitive constraints on ISPs are actually more substantial than for large edge providers in several market segments.[134/] Commenters agree that edge segments such as search, social media, operating system platforms, browsers, and online advertising are either dominated by a single player or highly concentrated.[135/] The record also reveals that switching between ISPs is no more difficult – and likely easier – than (1) switching email providers, which entails leaving behind one's email address; (2) switching operating systems, which likely requires a new device and leaving behind apps and software; or (3) switching to a new social network, which entails leaving behind potentially hundreds of connections.[136/] Companies

---

133/ T-Mobile at 11.

134/ NCTA at 47-48.

135/ *See, e.g.,* CTIA at 114-115 ("[I]n other service markets that comprise the broadband ecosystem, there is virtually no competition. For example, the market for operating systems comprises only two widely available providers (Android and iOS). In the online search market, one provider (Google) has more than 65% market share. And in the social networking market, Facebook has approximately 44% market share, as well as substantial other legacy advantages."); Thomas Lenard and Scott Wallsten, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking*, at 31 (May 2016) ("Lenard and Wallsten") ("Thus far, the market for digital advertising has been dominated by edge companies, such as Google, Facebook, and others who operate under the FTC's privacy enforcement regime."); USTelecom at 15 ("BIAS providers are small players in the advertising market and that their expansion in that market would increase competition and innovation. The $60 billion market for online advertising, primarily search and display, is dominated by large web and social media players, not ISPs. Search advertising, which represents approximately $29 billion, or 49 percent, of Internet ad revenues, is led by Google (64 percent), Microsoft (21 percent), and Yahoo (12 percent)."); T-Mobile at 10-11 ("One out of every five minutes on a mobile device is spent using the Facebook app. Sixty percent of all devices exchange traffic with Google every day, and twenty-five percent of all web traffic in North America runs through Google's servers.").

136/ *See, e.g.,* AT&T at 47; *id*. at 4 ("And it is ironic that the NPRM cites 'competition' as a basis for its proposed rules because, in fact, those rules would irrationally shield Google and other incumbents from competition by new entrants—ISPs—in the data marketplace."); T-Mobile at 11.

themselves recognize that switching providers of edge services is rare, which is why they pay exorbitant sums to be default providers.[137/]

Attempts to ground the Commission's asymmetric regime in studies of consumer behavior online are similarly misplaced.[138/] The Pew studies cited by the Commission and supporters of the proposed rules address consumer expectations across the entire broadband ecosystem, but do not identify any issues unique to ISPs that would support the disparate treatment embodied in the proposed rules.[139/] While expressing general concerns about the privacy of their information, the vast majority of consumers do not exercise options to modify the manner in which online entities use their data.[140/] And when consumers do take actions or express privacy concerns about specific entities within the broadband ecosystem, they are more concerned with the privacy of their data held by edge providers than by ISPs.[141/]

137/ ADTRAN at 8 ("The Commission's superficial analysis does not address the market power wielded by search engines and other edge providers. Indeed, regulators in Europe seem to believe that edge providers can wield anticompetitive market power. Moreover, if search engines can be changed 'instantaneously' as the Commission claims, then why do the search engine companies pay significant sums for the right to be the default provider? Google is reported to have paid Apple $1 billion in 2014 to be the default search engine for iPhones and iPads.").

138/ T-Mobile at n. 27 ("The Pew studies are not specific to BIAS providers; they also address the activities of edge providers such as Google and Facebook, which the NPRM does not cover. Moreover, the studies do not provide the granularity necessary to support the specific proposals here. Rather, they express merely the general (and utterly unsurprising) view that customers place some value on their privacy"); Comcast at n. 192; CenturyLink at n. 29; Verizon at 25-26.

139/ T-Mobile at n. 27; CenturyLink at n. 29; Consumers' Research at 15-16.

140/ Consumers' Research at 15-16 ("However, the Pew Report does not provide direct insight into customers' reasonable expectations about BIAS providers at all. That study shows that while privacy is important to consumers 'the vast majority of respondents—91%—had not made any changes to their Internet or cellphone use to avoid having their activities tracked or noticed.'").

141/ Electronic Transactions Association at 3 (citing Harvard Business Review study showing "73 percent of consumers surveyed said that telecommunications carriers were 'trustworthy' or 'completely trustworthy' when it came to making sure that personal data was never misused"); Consumers' Research at 7 ("Taking drastic regulatory measures against ISPs is unjustified, as studies show that ISPs are not the source of consumers' Internet privacy concerns. To the extent some consumers fear how personal information will be used online, those fears often center on edge providers, like search engines, online video sites, and social media sites."); *id.* at 15-16 ("Where consumers had revealed strong privacy

Notwithstanding claims to the contrary,[142/] NTIA's recent study does not actually demonstrate that privacy concerns will lead to lower broadband adoption.[143/] Indeed, NTIA itself has found that "less than one percent of those who do not use the Internet cited privacy as the main reason they stay offline."[144/] Further, to the extent that any perceived lack of trust impacts Internet use, that is an ecosystem-wide problem that will not be solved by an asymmetric regulatory framework that subjects consumer data to vastly different privacy regimes depending upon the identity of the broadband entity interacting with their data.

C. Adoption of the FCC's Proposed Rules Would Harm Consumers and Competition

Commenters warn that adoption of the proposed rules will harm consumers and competition in several key respects. First, the asymmetric regulatory framework for broadband consumer data is likely to confuse, rather than benefit, consumers.[145/] The record is bereft of any empirical data demonstrating that consumers favor subjecting ISPs to a more restrictive and granular set of constraints on their use of customer data than large edge providers like Facebook,

---

preferences through action, many of those actions related to edge providers or others in the Internet ecosystem—not necessarily to ISPs."); Comcast at 34-42.

142/ CDT at 20, n.26; EPIC at 29-30.

143/ Lenard and Wallsten at 19-20 ("There is little connection between privacy concerns and adoption."); Comcast at n. 192; Competitive Carriers Association at 9 ("A recent study reports annual wireless data traffic has grown threefold since 2013, and the estimated amount of wireless subscriber connections is near million, an all-time high. This suggests Americans are more invested in their wireless services and providers than ever before, and any anxiety related to privacy has not dampened interest, overall.").

144/ U.S. Dep't of Commerce, Nat'l Telecomms. & Info. Admin., *Exploring the Digital Nation: Embracing the Mobile Internet*, 37 (Oct. 2014), *available at* https://www.ntia.doc.gov/files/ntia/publications/exploring_the_digital_nation_embracing_the_mobile_internet_10162014.pdf ("*Exploring the Digital Nation*").

145/ AT&T at 56-58; Comcast at 43-44; Mobile Future at 7; Consumers' Research at 14; MMTC at 5-6.

Google, or Amazon.[146/] A recent survey of Internet users by Public Opinion Strategies and Peter D. Hart showed that by "an overwhelming 94%-5% margin, Internet users agree that 'All companies collecting data online should follow the same consumer privacy rules so that consumers can be assured that their personal data is protected regardless of the company that collects or uses it."[147/]

A variety of civil rights and public interest groups warn that a "patchwork of inconsistent, uneven data protection regimes would leave our constituencies in the precarious position of being protected from privacy abuses and data discrimination in some online contexts, while leaving people of color – and all consumers for that matter – exposed in others."[148/] Because of the disparate standards enshrined by the Commission for online consumer data, some consumers may mistakenly believe that declining to opt-in with their ISP protects their data against disclosure to third parties across the Internet, and thereby be less vigilant with respect to how their information is used by others in the ecosystem that would not be required to offer an opt-in choice prior to data collection and use.[149/] The end result could be a net reduction in privacy protection for consumers.

146/ Free State Foundation at 3; ITI at 8 (noting that the NPRM "contains no indication that consumer interests – in particular whether they are suffering harm under the current regulatory approach – demand expansive new regulations in this area"); Comcast at 5-6.

147/ Progressive Policy Institute, Internet User Survey at 2.

148/ NAACP, LULAC, et. al, at 2; *see also* LGBT Technology Partnership at 2-3.

149/ Consumers' Research at 14 ("[T]he uneven ecosystem may lead consumers to assume that the FCC's restrictions apply to all online activity. . . This incorrect assumption may cause consumers to be less vigilant online, which will weaken privacy and security rather than strengthening it."); NCTA at 53-55; MMTC at 3-7; LocationSmart at 2 ("Establishing a new set of rules that results in disparate user experiences, privacy policies and terms of use will only confuse end users and stifle innovation. We fear that such a scenario will lead to duplicative and potentially conflicting requirements on the providers of the affected applications and services, reducing the likelihood of their proliferation and continued development, and increasing the likelihood of misapplication or non-compliance with those policies simply due to the confusion and uncertainty that may be created.").

Second, the proposed rules will deprive consumers of beneficial uses of their data.[150/] The severity of the proposed rules reflects an underappreciation of the consumer benefits associated with data- driven capabilities, services, and offerings from ISPs. As ITIF writes, "The proposal does not seem to anywhere recognize the benefit of BIAS providers as an important source of useful data, and instead only seeks comment on how that data source should be restricted."[151/] While maximizing consumer welfare necessitates fashioning rules that balance the risk of privacy harms associated with various ISP data uses against the benefits of such uses, the Commission inexplicably fails to engage in such analysis.[152/] For example, the FTC Framework afforded ISPs the same opportunity as all other broadband entities to use data to tailor products, services, marketing, and advertising to their customers, thereby making such offerings more compelling for consumers while helping to defray network costs that would otherwise be recovered differently.[153/] As AT&T notes, by "making it far more difficult for ISPs to do what the rest of the Internet has long done—use nonsensitive customer data to engage in socially productive first and third-party marketing—the rules would reduce the profitability of

---

150/ NCTA at 44, 77-83.

151/ ITIF at 9.

152/ *Id.* at 9-10 ("Consumers generally benefit from the ability of BIAS providers to more effectively use data, both directly from, for example, enjoying more relevant, less intrusive advertising, and indirectly from having advertisers pay more of the network costs. As long as consumers can opt out of these practices, which, as we note above, they already can, this is win-win, not a violation of a supposed fundamental right of privacy. By not exploring the current and potential benefits of using data from BIAS providers before issuing new regulations, the Commission risks creating unintended consequences for consumers and the economy."); ICLE at 18 ("But the Commission's proposed rules fail to perform even a rudimentary cost-benefit analysis."); T-Mobile at 13-14.

153/ ITIF at 8-9.

broadband services, exert upward pressure on broadband prices, and depress incentives for broadband deployment."[154/]

Neither the Commission nor supporters of the proposed rules articulate how consumer welfare will be enhanced by making it harder for ISPs to utilize data to improve the products, services, and capabilities they offer their customers.[155/] The Association of National Advertisers (ANA) notes that a study of a similarly restrictive permissions regime with respect to online advertising in the European Union cost the European economy $1.4 billion each year.[156/] And the U.S. Chamber of Commerce points to Moody's Investor Services prediction that the NPRM will be "credit-negative" for ISPs, thereby threatening the data-driven marketing industry that "led to a $202 billion revenue increase to the national economy and created nearly 1 million jobs in 2014."[157/] Former FTC Commissioner Joshua Wright warns, much "of the innovation that routinely occurs in today's online ecosystem is a direct result of the very data uses the NPRM would curtail."[158/] Consumers' Research summarizes the impact on consumers as follows: "The FCC's proposal will degrade user experiences, deter practices that benefit consumers, and swamp consumers with useless information."[159/]

154/ AT&T at 4, 52-56; Wright at 18-22; ICLE at 5 ("The net result of these rules is that, on the margin, consumers will be presented with a narrower range of pricing and product options, meaning that fewer consumers — who have a wide range of heterogeneous preferences — will be offered their preferred options. Consumer welfare will consequently decrease."); Lenard and Wallsten at 26 ("If the default is opt-in, then information is lost—it does not flow to its highest-valued uses. This loss of information is costly and leads either to price increases as firms attempt to compensate for the loss of information or elimination of services.").

155/ *See* AT&T at 52 ("[I]f the government now imposed on the Internet ecosystem at large the type of notice-and-consent rules the NPRM contemplates here, it would slam the brakes on the modern Internet ecosystem, causing the economy incalculable damage in the process."); ICLE at 18; ITIF at 17.

156/ ANA at 21-22.

157/ U.S. Chamber of Commerce at 6-7.

158/ Wright at 25.

159/ Consumers' Research at 2.

Third, the Commission's proposal will harm competition. As NCTA explained in its initial comments, the default opt-in regime proposed by the Commission will deter ISPs from competing with the handful of large edge providers that currently dominate the online advertising market.[160/] Commenters echo the relative paucity of competition in online advertising and warn that the Commission's proposal will deter new entry into that market.[161/] As Comcast notes, "since ISPs are some of the few companies with the resources to enter this market… reinforcing the market power of these non-ISP incumbents… would essentially ensure that online advertising prices remain artificially high."[162/] Economists Thomas Lenard and Scott Wallsten observe that the asymmetric regulation fostered by the Commission would "put ISPs at a competitive disadvantage in the large and growing digital advertising market," create "an entry barrier to ISPs" that constrains their access to a revenue stream that defrays their network and operational costs, and thwart "new ISPs from using advertising . . . to offset consumer prices."[163/]

Given the importance of data-driven insights, capabilities, and offerings to companies that seek to enter the Internet ecosystem, the restrictiveness of the Commission's proposed

---

160/ NCTA at 58-59.

161/ ADTRAN at 9 ("[T]he Commission is making it more difficult for BIAS providers to compete against edge providers and search engines for advertising revenues, and so BIAS providers will have less money to invest in broadband deployment."); ANA at 4 ("BIAS providers are major advertisers that could be significantly disadvantaged in the interest-based advertising market by the FCC's proposal, resulting in widespread content and revenue loss and less effective and relevant advertising to the public."); ICLE at 12 ("[E]mpirical research shows that opt-in privacy rules reduce competition by deterring new entry. The seemingly marginal costs imposed on consumers by requiring opt-in can have a significant cumulative effect on competition."); Future of Privacy Forum at 14 ("The FCC should promote competition in the online advertising market, thereby enhancing the opportunities for publishers of every size to succeed. Currently, five companies—Google, Facebook, Microsoft, Yahoo and AOL—lead the market in online advertising, bringing in 61% of total domestic digital ad revenue in 2014. In the online services market, Facebook and Google account for 67% of mobile advertising, with social advertising comprising 70% of all of the revenue growth in display advertisements.").

162/ Comcast at 10; *see also* Lenard and Wallsten at 33 ("[J]ust as the FCC would (and should) be loath to discourage entry into the ISP market regardless of its views on the state of competition, it should similarly avoid increasing the cost of entry into digital advertising.").

163/ Lenard and Wallsten at 3.

regime also is apt to deter the emergence of new competition to ISPs because of the complexity of the rules and the manner in which they stifle data-related business opportunities. ITIF provides an overview of a number of potentially innovative and novel means by which alternative forms of competition to ISPs could emerge from software-defined networking, virtualization of network functionality, social media and cloud-based platforms, while warning that the stringency of the Commission's regime could "discourage potential new entry in network provision by historically data-center-focused companies."[164/] CALinnovates notes that "if a startup is a BIAS provider and offers other products or services empowered by customer data it will be subject to at least two different privacy regulations regarding the same consumer data depending on the type of product and services it is providing."[165/] Such a circumstance "discourages companies that are startups from entering the BIAS market, thereby decreasing competition."[166/] The proposed privacy rules continue a trend in which the breadth and severity of Commission regulation reduces the attractiveness of investment and competitive entry in the broadband service marketplace.

III. THE RECORD CONFIRMS THAT THE PROPOSED RULES ARE DEFECTIVE IN SEVERAL KEY RESPECTS

A. The Scope of Data Subject to the Proposed Rules Is Unnecessarily and Harmfully Overbroad

A wide range of commenters express alarm over the massive and unprecedented volume of data that would be subject to the privacy and security rules proposed in the NPRM, and its potential for interfering with basic Internet functionality and consumer expectations. The

---

164/ ITIF at 7-8; Lenard and Wallsten at 35 ("Making another source of revenue unavailable to ISPs may also block future entry" by companies trying to "offer service without direct payment by the end use.").

165/ CALinnovates at 6.

166/ *Id.*

Internet Commerce Coalition notes that the Commission proposal "covers a broad swath of information that is not in the least sensitive" and sweeps in "information that travels widely across the Internet whenever a user communicates."[167/] The Internet Advertising Bureau (IAB) observes that the scope of information covered by the rules "sweep[s] in new data types not traditionally included [as PII], a change that could have a broad negative impact on the Internet marketplace."[168/] While the Commission erroneously claims that its proposal incorporates the "modern understanding of data privacy," the Computing Technology Industry Association (CompTIA) correctly recognizes that the NPRM in fact defines PII "in a manner that does not comport with any prior definition of the term."[169/]

As NCTA noted in its initial comments, the breadth of information subject to the proposed rules includes data elements that are fundamental to basic network operations and service provisioning, such as IP addresses, domain information and device identifiers.[170/] Other commenters agree that by tethering these data elements to a rigid permissions regime,[171/] the

---

167/ Internet Commerce Coalition at 13-14; Future of Privacy Forum at 3 ("The current proposed rules define proprietary information very broadly — excluding all but the most high-level aggregate data — and then apply a single rigid framework to that information."); Messaging Malware Mobile Anti-Abuse Working Group (M^3AAWG) at 2 (noting the "extraordinary breadth of the data elements that the FCC proposes to include in the definition of 'customer proprietary information (CPI) subject to the rules, including IP address, MAC IDs and domain information").

168/ IAB at I; *see also* Advertising and E-Commerce Coalition at 6-7 (noting that treating as PII data elements which cannot, on their own, identify a specific individual - such as application usage data, geo-location information, and Internet browsing history – is "out of step with current privacy standards").

169/ CompTIA at 2.

170/ NCTA at 59-65 and Appendix A.

171/ Even the FTC recognizes that, absent Commission modification of its stringent permissions regime to more closely resemble the FTC's approach of subjecting only "sensitive" data uses to opt-in, it becomes more "necessary to revisit" and address the breadth of data subject to the proposed rules. *See* FTC Staff at 7, n.27; *see also* Ohlhausen June 8 Speech at 8 (noting that "IP addresses, are not sensitive by themselves. Under the FTC's approach, such non-sensitive PII about adults does not typically require heightened privacy protections such as opt-in consent. But under the FCC's proposal, an ISP would have to get opt-in approval for most uses of non-sensitive PII. Staff therefore notes that if the FCC rejects FTC

proposal would interfere with the continued seamless provision of network functionality and capabilities enjoyed by consumers today.[172/] CTIA echoes this concern, explaining that by "shoehorning tremendous amounts of relatively anodyne information into the category of 'customer proprietary information,' the Proposed Rules would cause massive disruptions in routine ISP operations."[173/] Likewise the Competitive Carriers Association notes that "the definition of 'customer PI' is extraordinarily and overly broad," and that such overbreadth renders many of the rules proposed in the NPRM "unworkable for providers."[174/]

Parties with IT, network engineering, and security expertise express particular concern with regard to the Commission's proposal to treat as CPNI and/or PII data elements as IP addresses, MAC IDs, and domain information which cannot, on their own, identify specific persons. The Information Technology Industry Council (ITI) notes that the permissions regime proposed in the rules encompasses use of IP addresses, device identifiers, and other data

---

staff's recommendations and subjects even non-sensitive PII to opt-in requirements, 'it may be necessary to revisit FTC's staff's proposed definition of personally identifiable information'").

172/ *See* Feamster at 1 (The FCC's proposal "raises significant concerns for (1) operators of ISP networks, who rely on network data to manage and secure their networks" and that as written the proposal "would harm" ISPs); *id.* at 8 ("ISPs collect, use, and share a variety of network data to operate and secure their networks. . . . Requiring notification and opt-in for many of these datasets would hinder network operations and research"); Audience Partners at 11 ("It is inappropriate and potentially detrimental to individual privacy rights to develop a bright line rule designating IP addresses as PII. IP address blocks and individual device IP addresses are necessarily collected and used for the basic functioning of the Internet"); *see also* Comcast at 77-81.

173/ CTIA at 130; Verizon at 3 ("The Commission's proposed definition of customer proprietary information is too broad and would lead to absurd results."); DMA at 5 ("By defining the regulated information too broadly, the NPRM creates nonsensical results."); AT&T at 34 ("[T]he proposed rules defy common sense because they would treat nonsensitive information categories . . . as though they were in fact highly sensitive data. No other agency has ever treated such information that way under any other U.S. privacy regime.").

174/ Competitive Carriers Association at 12-13; Consumers' Research at 10 ("The NPRM proposes to vastly expand the categories of information subject to the FCC's privacy jurisdiction—including even benign data like service plan information and traffic statistics—and considers rigorous access controls on such information. The result is to stifle the ability of ISPs to speak freely with their customers about their services and to limit consumers' access to information needed for routine transactions.").

elements that are not, on their own, identifiable.[175/] As a result, the "potential unintended consequences of these overly and unnecessarily broad definitions are quite concerning, particularly since many of the types of data captured by the proposed definitions are integral to providing Internet services to consumers, including securing Internet transactions."[176/]

While CDT contends that packet header information such as IP addresses, MAC IDs, domain information and URLs, and other metadata should be categorically defined as customer proprietary information (CPI) subject to the privacy rules' permissions regime,[177/] it disregards the consequences of such a decision in terms of basic Internet functionality.[178/] As security specialists Farsight Security observe, if "a provider is prohibited from 'disclosing' a customer's IP address to third parties, how will networking work? Providers need to be able to work with IP

175/ ITI at 13. EFF's suggestion that IP addresses should be automatically considered CPNI because they identify individuals, EFF at 3-4, contrasts sharply with positions it has taken elsewhere. *See, e.g.*, "Why IP Addresses Alone Don't Identify Criminals," August 24, 2011, https://www.eff.org/deeplinks/2011/08/why-ip-addresses-alone-dont-identify-criminals ("[I]n many situations, an IP address isn't personally identifying at all"); Dana Liebelson, *Why It's Getting Harder to Sue Illegal Movie Downloaders*, MOTHER JONES, Feb. 17, 2014, http://www.motherjones.com/politics/2014/02/bittorrent-illegal-downloads-ip-address-lawsuit.

176/ ITI at 13; *see also* Bennett at 8 (Classifying IP addresses and domain names as CPNI is "irrational because this information is available to websites and other Internet applications by the nature of the Internet. Without the sharing of IP addresses there is no communication across the Internet."); Letter from Mark Buell, Regional Director, North America, Internet Society, WC Docket No. 16-106 (June 2, 2016)(questioning NPRM's characterization of IP addresses and expressing concern that it could have "a negative effect on the global development of the free and open Internet").

177/ CDT at 12-15.

178/ *See* Deepfield Networks at 2, 5 ("IP address, ports and DNS responses—provide[] critical telemetry on traffic flows, quality, and trends that support daily Internet engineering. . . . Implementing a complex opt-in or opt-out regime for some CPNI data could significantly disrupt basic traffic engineering and service assurance capabilities used in all networks today."); IAB at 9 (Defining IP addresses, MAC IDs, application usage data, location information "as PII would fundamentally reshape how companies provide the free and low cost content that consumers have come to expect."); Bennett at (Classifying destination IP addresses as CPNI that presumably cannot be shared without affirmative consent of the customer "will not work.").

addresses for the Internet to work."[179/] As CALinnovates notes, this problem is particularly acute in circumstances in which an ISP is simultaneously providing BIAS and non-BIAS services in connection with the same broadband transmission.[180/] Nominum, a provider of DNS software, questions the validity of classifying DNS information as CPNI, noting that such classification could end up "exposing consumers to unnecessary risks and detracting from their overall Internet experience."[181/]

The sheer volume of data that ISPs would be obligated to protect in comparison to all other entities in the broadband ecosystem is apt to have competitive consequences as well – while providing nothing in the way of material privacy gains precisely because there is no constraint on the use of such information by the myriad edge providers that will continue to have access to it.[182/] ANA observes that ISPs "automatically share with websites" non-sensitive CPI data elements like IP addresses and traffic statistics and that imposing an "opt-in consent for all uses of non-sensitive customer information would have particularly drastic competitive

---

179/ Farsight Security at 6; Comments of the Security and Software Engineering Research Center at Georgetown University ("S^2 ERC Comments") at 7 (ISPs "must transmit IP addresses as a component of Internet service – otherwise, the service simply does not work.").

180/ CALinnovates at 5 ("In some cases where a company offers BIAS to customers along with other services the FCC's proposed Rule will force companies to simultaneously satisfy two different sets of privacy rules. CALinnovates believes that applying two privacy schemes to a company based on the services offered – rather than based upon the sensitivity of the data is not beneficial to either startups or consumers."); *see also* NCTA at 61-65 and Appendix A.

181/ Nominum at 4, n.9. Similar concerns arise with regard to automatically classifying location data as CPNI. Deepfield Networks at 5 ("One illustrative example is consent for collecting geo-location data. The NPRM proposes to consider information related to the physical or geographical location of a customer or customer's device, regardless of the particular technological method a BIAS provider uses to obtain this information, to be CPNI in the broadband context as it has been considered in the telephone context. However, this comparison does not appear to consider the fact that the location of a customer is absolutely necessary to route information to the appropriate servers and networks").

182/ Cloudmark at 6 (noting that IP addresses and other packet metadata classified as CPNI "are generally available to third parties other than the BIAS providers" and that the Commission's proposal "would unfairly regulate BIAS providers" use of such data while "other third parties with access to the same CPNI information . . . will not be subject to the restrictions detailed" in the *Notice*).

consequences for advertising, including BIAS providers that participate in the digital advertising ecosystem and other advertisers that would be adversely affected by the NPRM."[183/] AT&T notes that "ISPs must disclose each customer's IP address to every website that he or she visits" and that the "ISP cannot possibly be expected to constrain how all those millions of websites treat that information."[184/]

Assertions that ISPs "in principle" have the ability to link IP addresses with name and address information in no way demonstrates that edge providers lack that ability.[185/] More importantly, it misses the key point: the Commission is not proposing to require ISPs to seek approval to use or disclose IP addresses for non-BIAS purposes when such information *is* actually linked to subscribers' name and address information. It is, instead, proposing to bind IP addresses to the proposal's permissions regime *irrespective* of whether they are linked to subscriber names and addresses – and it is that massive overbreadth which renders the regime unworkable and harmful.[186/]

183/ ANA at 23-24.

184/ AT&T at 77; Deepfield Networks at 3 (noting that because Internet operations depend upon the sharing of CPNI data elements between ISPs, websites, and third party service providers, there are "simply too many necessary intermediaries involved at any given moment. Given the inherent use of CPNI data in Internet service delivery, the Commission must be aware that sharing data with third party providers is absolutely 'necessary for broadband service.'").

185/ *See* Comments of Professors Nick Feamster, David Farber, Yan Chen, Doug Comer, and Jim Hendler, at 2. *Cf.* Cloudmark at 6 ("Consumer IP information is readily available to a service operator (such as Facebook or Google) whenever a direct connection is made to its server and this service operator may associate it with an individual; however, they will not be restricted in using this CPNI in the same way as the BIAS provider.").

186/ *See* Audience Partners at 12 (noting NIST's determination that an IP address, by itself is not "directly identifiable data" and averring that "a static IP address, without being linked to other information, does not identify an individual"); Farsight Security at 6-7 (noting that dynamic and carrier grade NAT IP addresses cannot, on their own, cannot be mapped to an individual customer and concluding that "a much more carefully-written description of specific constraints around IP address disclosure should be prepared, if this restriction is needed at all"); Email Sender and Provider Coalition at 6-7 (noting importance of IP addresses in connection with email service and combating spam).

Commenters also recognize that the harms engendered by the scope of data subject to the proposed regime are exacerbated by the vague and open-ended, catch-all "linkability" standard proposed in the *Notice*.[187/] The Commission proposes to include as PII "any information that is linked or linkable to an individual," a concept that T-Mobile correctly identifies as "essentially boundless" and possessing "no limiting principle."[188/] Several commenters note that the Commission's proposal shuns even the basic step – employed by the FTC and other Federal agencies – of using a "reasonableness" standard to cabin the scope of the linkability standard.[189/] As the FTC recognizes, the Commission's proposed "linkability" standard would "unnecessarily limit the use of data that does not pose a risk to consumers" and would restrict uses of data regardless of whether the ability to link such data to individuals "is practical or likely in light of current technology."[190/]

Commenters highlight the flaws associated with the Commission's proposal to exclude from the category of "aggregate data" any information that is "reasonably linkable" to a "specific device."[191/] As AT&T notes, "information about a device can raise privacy concerns only to the extent that it can in turn be linked to a person."[192/] M^3AAWG notes that while the data it works

---

187/ CompTIA at 3 ("Including the vague term 'linkable' in the definition vastly expands the scope of what could be considered PII well beyond information that could actually be used to harm customers. Further, there are countless statutes defining PII that do not use the "linked or linkable" standard, and we do believe it is actually 'well established' in this context as the Commission has claimed."); Marketing Research Association at 4 ("Depending on who you ask, just about any piece of data could be 'linked or linkable to an individual,' making everything PII.").

188/ T-Mobile at 20.

189/ CTIA at 39-40; CompTIA at 3; Future of Privacy Forum at 3; Software & Information Industry Association ("SIIA") at 11-12.

190/ FTC Staff at 9.

191/ Audience Partners at 14-15; *see also* IAB at 9-10 (Information linked to a device, rather than to a specific individual, is more "'privacy friendly' to consumers as it allows the industry to operate on a non-identifiable basis, and removes incentives to keep identifiable data.").

192/ AT&T at 69.

with to address spam, malware, botnets and other online threats can rarely, if ever, be linked to a specific individual, most of that data "may in some fashion be considered 'reasonably linkable' to a device."[193/] As a result, the data flows that M[3]AAWG depends upon for its anti-abuse work could be threatened by the Commission's proposal.[194/] Indeed, a number of commenters highlight the operational, consumer and societal benefits that flow from de-identified and aggregate data sets, and express concerns that these benefits would be curtailed if the proposed regime is adopted.[195/]

Parties to this proceeding agree with NCTA's view that the Commission's proposal harms both privacy and consumer welfare by discouraging – rather than encouraging – de-identification.[196/] The Internet Commerce Coalition states that the Commission "overshoots well-established FTC privacy and security guidance in regulating de-identified information that has not also been put in aggregate form. If data are adequately de-identified, they do not raise privacy concerns and do not also need to be aggregated to be exempt from privacy requirements."[197/] As CTIA observes, the NPRM disregards research and analysis from NIST, the FTC and others highlighting the benefits of de-identification and instead proposes rules that

---

193/ M[3]AAWG at 5.

194/ *Id.*

195/ NCTA at 56, 67-68, 81-82, 89; Bennett at 7 ("The NPRM's dismissal by omission of the benefits and requirements of Big Data – and the related issues of anonymization, aggregation, and protection of large data sets – is deeply disturbing."); Deepfield Networks at 2; Consumers' Research at 23-24; IMS Health at 3, 8-9.

196/ NCTA at 68-70.

197/ Internet Commerce Coalition at 14. IMS Health at 5 ("The FCC has unnecessarily narrowed the de-identification approach in its proposal by failing to provide a mechanism for the de-identification of individualized information. By focusing exclusively on how "aggregated" information can be de-identified, the FCC creates an approach that diverges from every other regulatory approach that exists in the United States, including all of the approaches identified by the FCC in the NPRM."); Leibowitz at 6 ("The FCC's proposal appears to confuse the FTC's guidance on the 'reasonable linkability' standard and the appropriate steps companies can take to minimize such linkability with a standard for aggregation, which is but one way to de-identify data."); Audience Partners at 20.

"would eliminate any incentive that companies may have to de-identify data."[198/] Consumers' Research warns that "consumers have the most to lose" from the Commission's "refus[al] to recognize the difference between de-identified data and sensitive data," and its elimination of "regulatory incentives for companies to de-identify."[199/]

Contrary to CDT's contention,[200/] a handful of outdated anecdotes describing poor de-identification practices do not justify imposition of a vague and overbroad "linkable" standard or rules that discourage devoting resources and capital to good anonymization practices. As ITIF points out, scholars and researchers have cautioned against "over-react[ing] to the risks of re-identification," because the risk that attempts to re-identify data will cause concrete privacy harms is slight, and the benefits to consumer welfare from innovative uses of anonymized data are significant.[201/]

B. The Permissions Regime Is Too Restrictive

A broad range of commenters concur that the FCC's proposal will unnecessarily and harmfully constrain beneficial uses of data to the detriment of consumers, competition and innovation. First, commenters agree with NCTA that the Commission proposal harms consumer welfare by failing to provide broader latitude for first-party uses of broadband customer data.[202/] The Commission jettisons the FTC's established approach of permitting ISPs to use data to engage in first-party marketing of other products and services that may be of interest to their customers without having to solicit customer approval. As the Internet Commerce Coalition

198/ CTIA at 40-41.

199/ Consumers' Research at 22.

200/ CDT at 9.

201/ ITIF at 18. Consumers' Research at 24 ("If the Commission is interested in promoting consumer privacy and security, it should incentivize practices that have clear benefits, like de-identification.").

202/ NCTA at 72-74; Internet Commerce Coalition at 4; T-Mobile at 31-32; Advertising and E-Commerce Coalition at 7-8.

notes, the Commission's approach would thus require ISPs to obtain opt-in consent to "market over the top content packages, alarm monitoring or energy control services," even though such offers "are commonplace and do not pose a risk to consumer privacy."[203/] Such strict limitations on first-party marketing will lead to "absurd results" according to CTA,[204/] and are out-of-step with recommendations from both the White House and the FTC.

The White House privacy framework stated that "companies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in-person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it."[205/] The FTC Privacy Report reached similar conclusions, which are reiterated in the FTC's comments in this proceeding. The FTC notes that the restrictiveness of the Commission's approach to first-party marketing "does not reflect" consumer expectations because "consumers may prefer to hear about new innovative products offered by their BIAS providers."[206/] Indeed, commenters emphasize that the Commission's approach to first-party marketing is even more

---

203/ Internet Commerce Coalition at 4.

204/ CTA at 8; *see also* Comcast at 50 ("How can it make sense to deny the ISP customers in the above examples the benefits of learning of new company offerings and potential attendant price discounts for the existing services the customer receives when the FTC and the Administration in its Consumer Privacy Bill of Rights have concluded for years that such marketing is within the clear expectation of ISP customers.").

205/ The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 17 (2012), *available at* https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

206/ FTC Staff at 22-23; *see also* Earth Networks at 6-7 (Requiring ISPs "to obtain opt-in consent to receive marketing offers, whether from the BIAS provider itself or from third parties, will eliminate the potential for many customers to receive more targeted offerings for services they might well desire to know more about, contrary to the stated intent of the NPRM.").

prohibitive than the EU General Data Protection Regulation, which does not require opt-in consent to use customer data for marketing or advertising their products to existing customers.[207/]

Second, a broad range of commenters agree that the Commission should abandon its default opt-in proposal, and instead reserve opt-in consent only for uses or disclosures of sensitive data.[208/] As several commenters point out, the Commission's proposal disregards a basic tenet of virtually every existing privacy regime in place today, which is that "customer expectations and preferences differ based on the sensitivity of the information used and shared."[209/] The survey placed into the record by the Progressive Policy Institute found that by a margin of 83%-12%, customers agree with the proposition that the protections afforded for broadband customer data should be predicated upon the sensitivity of the data.[210/]

The FTC's comments criticize the Commission's default opt-in proposal because it "does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data," and could therefore "hamper beneficial uses of data that consumers may prefer."[211/] Instead, the FTC recommends the Commission revert to "the FTC's longstanding approach, which calls for the level of choice to be tied to the sensitivity of data…"[212/] The FTC's summary of its recommendations states flatly that "opt-out is sufficient for use and sharing of non-sensitive data,"[213/] and numerous commenters echo this recommendation.[214/]

207/ CTIA at 122; Internet Commerce Coalition at 7-8.

208/ SIIA at 7-9; ITI at 14-15; Electronic Transactions Association at 13; Advertising and E-Commerce Coalition at 7-8; CompTIA at 7; ACA at 26; INCOMPAS at 12; USTelecom at 9-10.

209/ T-Mobile at 7; Internet Commerce Coalition at 9-13; ; ICLE at 2; ACA at 40.

210/ Progressive Policy Institute, Internet User Survey at 3.

211/ FTC Staff at 22.

212/ *Id.* at 23.

213/ *Id.* at 35; *see also* Leibowitz at 9 ("The FCC's overbroad opt-in approach has the potential to stifle innovation and competition in the online advertising marketplace, and undermine benefits to

As former FTC Commissioner Joshua Wright notes, the FCC's proposal presumes that consumers with strong privacy preferences cannot act effectively to protect themselves by opting out, while shifting the burden to act to consumers that do not have strong privacy preferences.[215/] The Commission's approach harms consumer welfare by misallocating the costs and burdens of decision-making regarding use of non-sensitive broadband data away from the minority of ISP customers who have strong preferences regarding how such information is used.[216/] Instead, those burdens will now be borne by the great majority of customers that already have demonstrated – via their behavior under the FTC framework – comfort with having non-sensitive data used by their ISP in order to receive customized marketing, advertising, and capabilities.[217/] Earth Networks, a provider of new home energy efficiency services, highlights the practical

---

consumers. As the FTC has recognized, the ability to effectively monetize online data has yielded astounding benefits. Consistent with the FTC's technology-neutral approach, broadband providers should be able to use information in a manner consistent with consumer expectations and in a way that correlates to how the rest of the Internet ecosystem provides choice - on an opt-out basis. Requiring over-inclusive opt-in choice would unduly restrict broadband providers from participating in the same Internet marketplace the FTC has found to provide benefits to both consumers and competition.").

214/ *See, e.g.,* ITI at 14-15 ("Experience shows that an opt-out or implied consent standard is an effective mechanism to effectuate consumer privacy preferences with respect to non-sensitive online data while allowing legitimate practices, including advertising, to continue. We urge the FCC to follow the FTC approach of permitting an opt-out approach for use of consumer data in most instances, with an opt-in approach reserved for uses of the most sensitive consumer data."); ITIF at 17 ("At a minimum, the FCC should do away with its broad opt-in requirement for use and sharing of data by BIAS providers. The United States has generally gone with opt-out privacy frameworks, and only applies opt-in requirements for especially sensitive information."); *supra* note 208.

215/ Wright at 17-18.

216/ Beales at 11 ("Default rules should be designed to impose the costs of transactions on consumers who think these costs are worth paying. An 'opt-out' default rule means that consumers who . . . care more intensely. . .will face the costs of making a decision. In contrast, an 'opt-in' default rule enables those who care the most about the issue to avoid the decision costs, because the default will match their preferences.").

217/ *See* Ohlhausen, at 3 ("If a regulation imposes defaults that do not match consumer preferences, it imposes costs on consumers without improving consumer outcomes.").

consequences of this unwarranted shift: consumers will have reduced opportunities to learn about innovative new products and services of significant potential value to them.[218/]

Parties that endorse the Commission's default opt-in proposal never explain how consumers benefit from a regulatory framework in which it is harder for ISPs to use data to provide relevant advertising and other customized offerings than other online entities with access to similar customer data.[219/] By disregarding data sensitivity and the propensity for uses of customer information to cause actual consumer harm, the default opt-in approach proposed by the Commission will adversely affect both consumers and competition.[220/] An opt-out approach for non-sensitive data would adequately protect the ability of consumers to exercise control over uses of their data, while giving ISPs more leeway to use data in ways that foster customization, innovation and lower costs.[221/]

Some parties erroneously suggest there is no harm from the Commission's approach because if consumers consider data uses presented to them to be beneficial, they will opt in.[222/] Considerable research, including studies highlighted by the Commission itself, demonstrates that defaults dictate choice outcomes for the majority of individuals.[223/] That tendency is particularly problematic here, because of the considerable social costs associated with the aggregate effect of

---

218/ Earth Networks at 6-7.

219/ *See, e.g.,* CDT at 23-24.

220/ *See* Ohlhausen, at 3 ("The burden imposed by a broad opt-in requirement may also have negative effects on innovation and growth."); Leibowitz at 9 ("The FCC's overbroad opt-in approach has the potential to stifle innovation and competition in the online advertising marketplace, and undermine benefits to consumers.").

221/ ITIF at 17.

222/ *See, e.g.,* Access Now at 6-11; ACLU at 8-9; EPIC at 4.

223/ *See* NCTA at 79, n. 294; *see also* Comcast at 48 ("[A]n opt-in consent mechanism results in far fewer individuals conveying their consent than is the case under an opt-out consent mechanism. In fact, a series of studies has shown that people faced with an opt-in choice almost never opt-in even where there are substantial benefits."); ICLE at 11-12; Lenard and Wallsten at 25-26.

individual decisions to not allow beneficial uses of non-sensitive data.[224/] Because defaults heavily influence decision-making, the practical effect of shifting to an opt-in default regime is to deprive broadband consumers of the benefits of data-driven offerings, thereby undermining consumer choice and stifling competition and innovation.[225/]

EFF's suggestion that predicating a permissions regime upon the sensitivity of data would create "a perverse incentive for BIAS providers to identify or inspect protected data in order to determine whether it falls into a "sensitive" category" is utterly without foundation.[226/] ISPs complied with the FTC privacy framework for years without manually inspecting every packet – even assuming such action was reasonably feasible. Further, Congress already distinguished between data sensitivity levels by forging legally operative distinctions between non-CPNI, CPNI that is individually identifiable, and CPNI that is not individually identifiable. If the Commission cannot craft broadband privacy rules that establish and effectuate distinctions between levels of data sensitivity, then that only further reinforces the incompatibility between the proposed rules and any existing statutory authority for them.[227/]

224/ Wright at 19-20; AT&T at 52-53 ("And in making that non-choice, individual consumers do not fully internalize the broader social costs of their nonparticipation in the information economy."); SIIA at 6 ("[T]he socially beneficial uses of data made possible by data analytics are often not immediately evident to data subjects at the time of data collection."); Lenard and Wallsten at 26-27.

225/ *See* Behavioral Economics Consulting at 2 (The proposed default opt-in regime "is not offering people more choice, it's offering them less – in effect, deciding for them."); IAB at 8 ("An opt-in regime will disrupt the data flows that fuel the Internet economy, and may ultimately prove to be less effective and responsive to consumer demands."); Comcast at 49 ("[B]y subjecting all but a small portion of ISPs' consumer data usage and disclosure activities to an opt-in requirement, the Commission would be stepping into the consumers' shoes and ensuring that ISPs will not be able to effectively inform consumers about products and services from which they could benefit."); Electronic Transaction Association at 13 (Mandating opt-in for use of non-sensitive data "would put broadband providers at a competitive disadvantage and may deprive their customers of the opportunity to realize the potential upside of the beneficial use of customer data for targeted advertising or other purposes.").

226/ EFF at 5; *see also* Public Knowledge at 24.

227/ *See supra* Section I.

Third, commenters agree that the enumerated exceptions to the permissions regime proposed by the Commission are far too narrow and will unnecessarily constrain beneficial activities that support consumers and promote competition and innovation.[228/] As NCTA noted in its initial comments, the vast range of data elements defined as CPI affect more than just provision of broadband Internet access service by ISPs. IP addresses, device identifiers, location information and other data elements proposed as CPI also are critical to fulfilling customer requests for non-BIAS services and capabilities that are integrated with (and provided simultaneously with) broadband transmissions such as email from an ISP account, DNS look-up, delivery of anti-virus software, streaming music or other online content.[229/]

Like NCTA, commenters raise concerns that the Commission's proposal could constrain ISPs from using CPI in connection with furnishing communications and services that a consumer wishes to send or receive via a broadband transmission.[230/] As CTA notes, "the complete and utter lack of clarity in and arbitrary nature of the proposed approval rules would undoubtedly have a chilling effect" on the ability of ISPs to develop and furnish (either alone or partnering with third parties) offerings and services over their networks.[231/] This uncertainty could force ISPs into launching campaigns of click-through agreements (which are likely to annoy and repel consumers) simply to obtain consents to provide customers services and capabilities they are accustomed to receiving today as part of their broadband Internet access service.[232/] This

---

228/ CTIA at 137 (While defining "the category of protected information . . . broadly," the NPRM also signals that its "exceptions are rigid and narrow."); Comcast at 59-60.

229/ NCTA at 74-76.

230/ CALinnovates at 5-6; NCTA at 3-4; Internet Commerce Coalition at 5.

231/ CTA at 9; Earth Networks at 4.

232/ CTA at 9.

outcome harms, rather than benefits, consumers by making it materially more costly and burdensome to continue providing offerings they enjoy today.

Apart from failing to make clear that its rules do not restrict uses of CPI that are necessary for, or incidental to, transmitting or providing services or capabilities customers have requested or purchased via their ISP, the exceptions for non-consensual uses of customer information proposed in the *Notice* fail to capture basic tasks and functionalities necessary to operate and manage broadband networks.[233/] T-Mobile notes that the proposed regime hinders the ability of ISPs to use "third-party vendors for a variety of functions essential for helping maintain the quality of service consumers expect," and that these limitations undermine efforts to "provide quality services through a seamless customer experience."[234/]

Commenters also question the efficacy of the exceptions afforded by the Commission for use of broadband customer data to share cyber threat information and combat abusive behavior.[235/] As M^{3}AAWG notes, the concerns with these exceptions arise because the "extraordinary breadth" of the Commission's rules implicates "data elements . . . central to our work, even though they do not inherently or automatically identify any specific person."[236/] This breadth, in combination with the relative narrowness of the proposed exceptions, raises

---

233/ Verizon at 64 ("The provision of broadband service includes and requires the ability to troubleshoot and resolve issues with the service; to maintain the safety, security, speed, and operability of the service; and to manage the broadband network. The Commission should take the opportunity to affirm that broadband providers may access and transmit customer information to third parties to fulfill these obligations.").

234/ T-Mobile at 32-33.

235/ NCTA at 76-77.

236/ M^{3}AAWG at 2. Email Sender & Provider Coalition at 3 ("If BIAS providers that offer email services are limited in their ability to share information about messages that consumers consider to be spam, the entire email ecosystem could suffer, and email senders would not just lose a significant part of valuable insights into why their messages were unwanted, but also unknowingly continue to send email to consumers that is unwanted by such consumers.").

significant concerns that important, ongoing efforts to fight spam, malware, botnets and other online exploitation will be curtailed or thwarted.[237/]

Similarly, ITI warns that the cybersecurity exception proposed in the NPRM "may not be nearly broad enough to adequately help protect the Internet ecosystem."[238/] As NCTA noted in its initial comments,[239/] the Commission's rules could interfere with beneficial cybersecurity information sharing sought to be encouraged under the recently-passed Cybersecurity Information Sharing Act (CISA).[240/] Under CISA, companies may, "notwithstanding any other provision of law," share cyber threat indicators (CTIs) for a "cybersecurity purpose."[241/] Under the FCC proposal, however, sharing of CTIs that include CPNI would be subject to a potential post-hoc determination of whether such disclosure is "reasonably necessary" to protect against cyber threats. The government's own CISA guidance documents for private companies anticipate the sharing of information that the Commission proposes to classify as CPNI, such as IP addresses and domains suspected of originating an incursion or being used as vectors of an attack.[242/] Thus, the Commission's approach will require ISPs to spend considerable time

---

237/ M^{3}AAWG at 2-6 ("[M]any of the techniques and tools utilized today to fight online messaging abuse are predicated on the successful sharing of data elements between ISPs and other internet services – be it other ISPs or third-parties – that are categorized as CPI in the NPRM. These data exchange models work because they allow security professionals to share data with minimal friction. The NPRM as it is currently written would add considerable friction to these tools and mechanisms, preventing the exchange of key information, and therefore would significantly impair the efficacy of these existing tools.").

238/ ITI at 14.

239/ NCTA at 76 and Appendix A at 27-29.

240/ The NPRM proposes to allow only sharing of CPNI – but not PII – necessary to protect against cyber threats. *Notice* at ¶ 117. It offers no explanation for this disparate treatment – and no acknowledgement that a prophylactic bar against sharing of PII was not adopted by Congress - but instead simply asks whether sharing of PII also should be included. *Id.*

241/ Cybersecurity Act of 2015, Pub. L. No. 114-113, Div. N., Title I, § 104, 129 Stat. 2242, 2941 (2015).

242/ Dep't of Homeland Security and Dep't of Justice, GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES

deliberating whether to share a key element of security information, which could have significant adverse consequences in a real-time attack situation.[243/] It also could discourage common cybersecurity-related uses of IP addresses that may not be considered linked to an imminent threat – such as sharing IP addresses with third-party security vendors and academic researchers studying threat vectors, tools performance, and threat intelligence capabilities.[244/]

It makes no sense for the Commission to develop privacy rules that have the potential to adversely affect measures and practices aimed at protecting the security of customer data.[245/] While Professor Feamster proposes a laundry list of explicit exceptions from restrictions on use of certain CPI for researchers, protocol developers, vendors, security specialists, network management and operations vendors,[246/] such an approach is, at best, only a partial solution – it will inevitably be incomplete.[247/] The heart of the problem is the Commission's insistence on

---

UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015, at 5-6 (June 15, 2016)("DHS/DOJ CISA Guidance").

243/ While CISA requires a company sharing CTIs to assess – or use a technical capability to remove – information not directly related to a cyber threat which the company "knows at the time of sharing to be personal information" of, or identifying, a specific individual, CISA, § 104(d)(2(A), the statute, unlike the Commission's proposal, does not automatically consider an IP address to be "personal information." Indeed, the government guidance documents contrast CTI observable characteristics such as IP addresses and URLs with "personal content or information inappropriate to share." DHS/DOJ CISA Guidance at 6. In addition, the "known at the time of sharing" standard negates the threat of after-the-fact second-guessing inherent in the Commission formulation.

244/ Feamster at 3-4 ("Preventing ISPs from collecting [IPFIX] data and sharing it with vendors of security services or researchers will harm the security and performance of the Internet and threatens to inhibit research innovation."); Comments of Manos Antonakakis, Georgia Institute of Technology, et. al. at 5-6 ("Security researchers often collect iterative DNS information in order to identify dynamic threats to networks or track online infections. As a simple example, consider… where the IP address of the University is resolved. It is quite useful to security researchers to observe instances when, for example, this IP address is changed to a malicious third-party host."); Email Sender & Provider Coalition at 6-7.

245/ *See, e.g.,* Nominum at 4-5; CTIA at 139-41; AT&T at 117.

246/ *See* Feamster at 7-8.

247/ *See, e.g.,* M^3AAWG at 2 (Enumerating exceptions for beneficial practices employed today "will still prevent the creation of new security techniques and mechanisms that leverage data sharing models not currently envisioned.").

subjecting non-sensitive data elements and data uses that do not implicate significant privacy risks to a rigid and inflexible permissions regime.[248/]

Fourth, commenters express concern that the new notice and approval solicitation obligations proposed by the Commission will disrupt the provision of service, frustrate consumers, and spawn notice fatigue.[249/] ANA states that the Commission's proposed approach is apt to make "opting-in to interest-based digital advertising simply unworkable:"[250/]

> BIAS providers would potentially have to use intrusive methods, such as pop-up notifications, to get customers' attention on each site they visit, many of which will be off the BIAS providers' web site. Customers who wish to provide consent might then have to navigate back to the BIAS providers' homepage, at which point they would have to click through disclosures prior to giving consent. Such disclosures would be lengthy and complex because BIAS providers would have to disclose all potential uses of the information sought and include ancillary explanations about the extent and duration of such consent. Few, if any, customers would be willing to endure this onerous process and if these types of choices proliferate, as is likely, consumer annoyance and opt-in fatigue will increase substantially over time. Customers, in fact, may become so numb to this constant barrage of choice notifications that they may refuse to opt in altogether.[251/]

248/ *Cf. id.* at 6 ("Many of the problems identified here would be mostly (or perhaps fully) negated if the NPRM made clear that data elements identified as CPI – such as IP addresses and domain information – can be used without permission in circumstances where they do not identify any specific person because that is how the vast bulk of the information covered by these examples is used today.").

249/ CTIA at 100 ("Far from informing and empowering consumers, however, the Proposed Notice Rules could require frequent and intrusive notices to consumers, increasing the risk that customers will experience notice fatigue and possibly fail to appreciate the most important notices that impact customer privacy."); T-Mobile at 40 ("The Commission's proposed obligations risk flooding consumers with multiple uncurated notices – a deluge that would inhibit rather than heighten consumers' ability to focus on actual unwanted or harmful uses of their sensitive data. This problem would become especially acute in light of the additional notices the proposed rule would require providers to send in order to use and disclose even non-sensitive data.").

250/ ANA at 20.

251/ *Id.* CenturyLink correctly notes that it also would be "impractical" if the Commission's proposed notice rules were read to "to require that a customer service representative read a BIAS provider's entire privacy notice to a prospective customer, including the laundry list of elements the Commission would require be included in that notice." CenturyLink at 20. Instead, the Commission should at most require that ISPs "offer information about how to locate and review the provider's privacy policy at the point of sale, whether in person, over the telephone, and through other means." *Id.* at 21.

A number of parties object to the idea of mandating that ISPs provide multiple, recurring "just in time" notice and approval solicitations, in addition to spelling out their privacy and data use practices in a privacy policy.[252/] The FTC staff agrees. Their comments note that the "most relevant time" for ISPs to solicit choice for data uses "is when the consumer signs up for service."[253/] Accordingly, as "an alternative to the FCC's proposed approach," FTC staff recommends that ISPs be allowed to present consumers with an opportunity to solicit choice for data uses "upon sign up."[254/]

C. The Data Security Requirements Proposed in the Notice Are Counterproductive

"[T]he Notice purports to espouse a general data security standard based on reasonableness that would largely be consistent with the FTC's current approach, the language of the proposed rule appears to contemplate a strict liability framework."[255/] While BIAS providers

---

252/ USTelecom at 12 (Just in time notice obligations "would be overly prescriptive and not consistent with how consumers anticipate receiving notices from their ISP. The immediacy of the notice and large scale of non-sensitive information that the Commission has swept into its term customer proprietary information would make any such "just-in-time" notice extremely burdensome for consumers. Furthermore, in requiring multiple notices subsequent to the first notice, the Commission would be failing to take into context the sensitivity of the information in use. Requiring immediate notice about the use of information that consumers would expect to be shared leads to notice fatigue where by consumers start to ignore the content of such notices making them ineffectual."); Deepfield Networks at 5 (The Commission's analogy to just in time geo-location opt-in requests "does not make sense when applied to lower level Internet traffic flows. It would be infeasible for BIAS providers to provide consumer choice exactly the same way as edge providers before routing traffic flows and similarly, it would be infeasible and overly burdensome to establish a regime that would require BIAS providers to slow service to ensure that they honor any opt-in or opt-out before making any transfers in this lower level traffic flow."); T-Mobile at 28-29; CTIA at 143-44; Comcast at 43.

253/ FTC Staff at 24.

254/ *Id.* at 25; *see also* Leibowitz at 10 ("When the FCC finalizes its rules, it should adopt a flexible approach, recognizing that companies often need to craft notices to consumers in new ways and through new channels to accommodate changing technologies and evolving consumer understanding of business practices.").

255/ CenturyLink at 32; Verizon at 66; AT&T at 79 ("Literally construed, this would make ISPs strictly liable for data breaches, no matter how reasonable the data security measures they adopted. Any strict liability rule would create arbitrary and perverse over-deterrent effects, suppressing productive uses of data without any cost-benefit justification.").

have strong incentives to keep sensitive customer data secure, a strict liability regime is unreasonable and counterproductive.[256/] The goals of any data security procedures are to identify, minimize, and manage vulnerabilities, but there are no procedures that can completely eliminate risk.[257/] A strict liability rule would foster over-deterrent effects that could impose staggering costs and hinder productive uses of data management resources uncoupled from any cost-benefit justification.[258/]

ISPs should not be deemed to violate the Commission's rules if they employ reasonable data security procedures but nonetheless fall prey to data exfiltration by a determined and sophisticated cyber foe. The FTC agrees. Recognizing that the FCC's proposed data security rule "would impose strict liability on companies for 'ensuring security,'" FTC staff instead suggests "modifying the language to require BIAS providers to 'ensure the reasonable security, confidentiality, and integrity of all customer PI.'"[259/] This is consistent with the standard that governed ISP data security standards prior to reclassification, and neither the Commission nor supporters of the proposed rules has offered any rationale for departing from that approach. While the Commission should heed the FTC's advice to abandon its strict liability standard, severe problems with the data security rules would still remain. As numerous commenters point out, the broad scope of data covered by the security mandate will require ISPs to devote considerable resources and personnel aimed solely at ensuring technical compliance with overbroad mandates to secure non-sensitive data, regardless of how efficient (or inefficient) such

---

256/ T-Mobile at 49.

257/ Verizon at 66 ("Data-security procedures are designed to minimize the risk of an attack. Even the best procedures, however, cannot completely eliminate that risk. On the contrary, a company may implement state-of-the-art technologies and still be the victim of an attack.").

258/ AT&T at 79.

259/ FTC Staff at 27.

resource deployments may be with regard to protecting against bona fide threats to sensitive customer data.[260/] The application of the data security and data breach obligations to a large spectrum of non-sensitive data routinely employed in connection with basic Internet function and operations – and routinely accessed by Websites, search engines, browsers, online advertisers and a host of other third parties – will create enormous compliance burdens and will harm consumers.[261/]

Most commenters also agree that the specific data security obligations proposed or considered in the *Notice* should not be adopted.[262/] They are overly prescriptive, not calibrated to incentivize protection for sensitive data, and inconsistent with state and federal policy.[263/] Imposing across-the-board mandatory risk management practices, robust customer authentication requirements for access to customer information, and maintenance of year-long logs of all access to or disclosure of the huge swath of data covered by the rules goes far beyond any existing data security regime.[264/] Adherence to a static set of prescriptive regulations will not effectively deter risks to data security,[265/] but commenters are clearly concerned that the volume and scope of specific data security requirements being considered by the Commission will grow and deepen.

260/ CTA at 10; AT&T at 75-76; CenturyLink at 35-36; CTIA at 150.

261/ As NCTA noted in its original comments, home wireless routers broadcast their SSID and MAC address to proximate devices of guests, and "in the clear" transmission of DNS request and IP address information by Wi-Fi networks could implicate compliance issues under the data security and breach notification rules proposed in the NPRM. NCTA at 92, n. 340, Technical Appendix at 24.

262/ *See, e.g.,* Comcast at 59-61, 64-66; State Privacy and Data Security Coalition at 4-5; FTC Staff at 27-30; Verizon at 65-69.

263/ CTIA at 146 ("The Commission's proposed approach to data security is not based on a firm grasp of network security, the complex Internet ecosystem, risk management, or sensitivity analysis. By applying and expanding rules for CPNI to virtually all information that ISPs handle, the Commission risks endangering security and stifling innovation.").

264/ State Privacy and Security Coalition at 11.

265/ *See* CTIA at 146.

T-Mobile highlights the problems with just one of the mandates being considered by the Commission:

> For example, the NPRM's discussion of authentication requirements asks whether the Commission should require multi-factor authentication, mandate password protection, and adopt specific authentication procedures for particular scenarios. This type of prescriptive requirement fails to consider the cost to the BIAS provider of implementing and operating such a system for authentication. It also does not consider the impact to the consumers who would need to understand the proper use and protection of secondary tokens or biometric data. In addition, distribution of tokens, protection of biometrics, and the additional protection of these types of secondary authentication mechanisms will create additional complexity for both the BIAS provider and the consumer.[266/]

The proposed rules also would require ISPs to conduct mandated risk assessments – which the NPRM envisions as being designed and dictated by the Commission – and to "promptly remedy any" security concerns that the assessments identify. Read literally, this would obligate ISPs to immediately address any issue identified in an assessment, regardless of materiality, cost, sensitivity of the data at risk, or risk of adverse consequences.[267/] The Commission proposal will shift ISPs from an agile, pro-active cyber defense posture focused on addressing the latest iteration of cyber threats and attack scenarios, to a backward-looking, checklist compliance stance.[268/]

266/ T-Mobile at 49.

267/ AT&T at 79. Likewise, the proposal also requires every ISP to designate a "senior management official with responsibility for implementing and maintaining" its security program, and goes on to raise the possibility of specifically delineating the qualifications for that position. While most ISPs have an established and delineated organizational structure for addressing security issues, that evolves organically and is typically tailored to the management structure and security needs and resources of each specific company. It is counterproductive for the government to be dictating to private companies how they should organize themselves to address security.

268/ Leibowitz at 11 ("The NPRM's requirements for risk assessments and audits of non-sensitive information divert resources away from protecting truly sensitive information and maintaining the security of networks.").

Commenters correctly recognize that such an outcome would be counterproductive for data security and directly in conflict with Federal policy.[269/] Imposing prescriptive requirements conflicts with the Federal preference for relying on voluntary mechanisms and industry-driven best practices to secure networks.[270/] In adopting the Cybersecurity Framework that constitutes the lynchpin of the Administration's cybersecurity policy for the private sector, the National Institute for Standards and Technology (NIST) rejected precisely the kind of "one-size-fits-all approach to managing cybersecurity risk" the Commission embraces here.[271/] NIST recognized that organizations "will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary." It also understood that organizations can and should "determine activities that are important to critical service delivery" in order to "prioritize investments to maximize the impact of each dollar spent."[272/]

Not only is the Commission's proposal inimical to the approach championed by NIST and the Administration, it also is in conflict with its own stated policies. Chairman Wheeler previously championed a "new paradigm" of "business-driven cybersecurity risk management" that eschews regulatory mandates and is instead governed by "private sector innovation."[273/] However, "without any evidence that industry has failed to meet its obligations in this area, the

---

269/ ITI at 2 ("[T]he prescriptive, inflexible data security requirements . . . are misaligned with current industry practice and federal policymaking."); CTIA at 154-158; DMA at 21-22.

270/ USTelecom at 21-27; ITI at 2; ACA at 32.

271/ *Framework for Improving Critical Infrastructure Cybersecurity*, Nat'l Inst. of Standards & Tech., at 2 (Feb. 12, 2014).

272/ *Id*.; State Privacy and Security Coalition at 11-12.

273/ Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute (June 12, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf.

FCC appears prepared to abandon the new paradigm in favor of the old regulatory paradigm that it acknowledges will not work."[274/]

The record provides no reasonable justification for the Commission's proposed reversal of course. To the extent the Commission can lawfully adopt any data security requirement, it should do no more than mirror the general "reasonableness" standard successfully employed for years by the FTC.

D. The Proposed Data Breach Rules Are Unworkable

Commenters agree that the definition of breach is too vague, the scope of data subject to the notification obligation is vastly overbroad, and the absence of any "harm" qualifier on the notification obligation is unreasonable, out-of-step with other data breach laws, and will create notice fatigue.[275/] As the State Privacy and Security Coalition writes:

- No state breach notice law requires securing or providing breach notice about information that is simply linked or linkable to an individual, much less of IP addresses or MAC addresses.[276/]
- There is no harm trigger for the breach notice required by the FCC, unlike in 41 states.[277/]
- Unlike every state law, the proposal would require notification: (1) in all cases to the Commission within seven days and to individuals within 10 days, (2) even if the customer data were encrypted or otherwise protected; (3) even if an employee or contractor accidentally accessed customer information for a legitimate business purpose in excess of authorization; and (4) even if an employer or contractor had the right to access the system, but did so in a way that exceeded permissions in company policy. These requirements are far more stringent than any existing data breach regime.[278/]

274/ USTelecom at 26.

275/ *See* NCTA at 90-93; Internet Commerce Coalition at 15; ITI at 11-12; Verizon at 68-69.

276/ State Privacy and Security Coalition at 11.

277/ *Id.* at 12.

278/ *Id.*

- Unlike 44 state breach laws, the Commission proposal would require notice even if the unauthorized person simply accessed the system and did not copy or download any material from it.[279/]

The FTC recognizes that the capacious scope of data subject to breach notification would reduce privacy and security by effectively requiring that ISPs maintain all information about consumers in identifiable form.[280/] FTC Staff recommends that the Commission reduce the scope of data subject to a breach obligation, since the rule as drafted would require notification to consumers even in circumstances in which only non-sensitive information was affected.[281/] This over-notification would lead to notice fatigue as "the inevitable result of the Commission's proposal is that customers will receive notifications that they do not care about and that create unnecessary confusion and anxiety, such that customers could stop paying attention to notices altogether and miss those that might actually be important."[282/] This is why most states include a harm trigger, provide an encryption exception, and carve-out any de-identified data.[283/]

279/ *Id.*

280/ FTC Staff at 31 ("The first concern is that because the definition includes unauthorized access to any customer proprietary information, companies that only collect data such as device identifiers or information held in cookies may be required to collect other consumer information such as email addresses in order to provide consumers with breach notification.").

281/ *Id.*; Verizon at 68; State Privacy and Security Coalition at 9; XO at 8 ("There is no existing data breach notification standard in the United States that is this broad or ambiguous. And the consequences of such an open-ended definition that is not based on sensitive data would inevitably result in a flood of breach notifications, even if only non-sensitive and un-linked information is accessed."); NCTA at 91-92.

282/ Verizon at 69; *see also* DMA at 16 ("The Commission's expansive definition of PII could trigger breach notification obligations for types of data that have not been captured under state and other federal regulatory regimes that have evaluated the types of information that warrant breach notification. As a result, consumers would face over-notification and risk becoming desensitized to such notices."); Internet Commerce Coalition at 15(the rules "could cause consumers to ignore more serious breach notifications."); FTC Staff at 31-32; ITI at 11.

283/ State Privacy and Security Coalition at 12-13, 16.

Commenters also agree that the short 7-10 day timeline is unprecedented and unworkable.[284/] The Direct Marketing Association notes that "no data breach notification law or regulation has a requirement for notification to consumers no later than 10 days after the discovery of the breach, as the Commission is proposing."[285/] The FTC proposes adoption of a 30-60 day timeframe for notice,[286/] more in line with state breach notification laws that average 45 days when a specific timeline is included at all.[287/] Alternatively, XO notes that "nearly all state laws provide that companies must notify affected consumers 'in the most expedient time possible and without unreasonable delay' or similar language that considers the time necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[288/] The FTC comments and state data breach laws recognize that companies need time to ascertain the extent and potential impact (if any) of the breach, engage with security specialists and forensic firms, and undertake a thorough and accurate investigation to minimize the prospect of unnecessary or inaccurate notifications.

The National Retail Federation ("NRF") laments "notice holes" associated with breaches of ISP transit networks in state and federal law, due to language that may exempt or limit breach notification obligations for third party service providers in some circumstances.[289/] But there is a good reason for that. Third-party service providers are typically not well-positioned to furnish a breach notice to the customers of the entity for which they are storing or transporting data,

---

284/ *See, e.g.,* NCTA at 93; XO at 12; FTC Staff at 32-33; State Privacy and Security Coalition at 13-15.

285/ DMA at 25.

286/ FTC Staff at 33.

287/ XO at 13.

288/ *Id.*

289/ National Retail Federation at 3-6.

because they are not in privity with those customers.[290/] For service providers like ISPs engaged in data transport the constraints on providing notice are particularly problematic. As NCTA noted in its initial comments, ISPs transport enormous amounts of traffic over their networks each day without knowing or inspecting the contents of those communications and a considerable amount of such traffic is originated by or sent to users with whom they have no customer relationship.[291/] ISPs today do not filter traffic in order to warehouse identifying information in anticipation of providing notices of potential future breaches of data that they handle on a transient basis. In order for carriers to know whether CPI in transit was affected by a breach, they would need to overlay massive apparatus to monitor, log and store information concerning all traffic transiting their network – whether from their own subscribers or from senders and recipients of data that utilize other service providers.[292/] This would impose extraordinary capture and storage costs, potentially engender filtering delays in handling Internet traffic, and set the stage for precisely the type of comprehensive, content-based logging and warehousing of Internet traffic the Commission and privacy advocates seek to avoid in other contexts.[293/] As even Professor Feamster acknowledges, ISPs do not have the kind of panoptical

---

290/ Indeed, imposing such an obligation would implicate the transfer of such customers' personal information from the first party to the third-party service provider.

291/ NCTA at 91, n.337.

292/ *Cf.* FTC Staff at 31 (As a result of proposed data breach rules, ISPs "may be required to collect *other* consumer information" in order to meet breach notification obligations.); State Privacy and Security Coalition at 9 ("The proposed rule likewise effectively requires implementing audit logging in order to account for each event of access to or disclosure of the broad categories of CPNI and customer proprietary information to third parties.").

293/ *Cf.* Public Knowledge at 24-25 ("Placing a requirement on broadband providers that would result in them viewing more details about a customer's communication in the name of privacy is, to put it mildly, self-contradictory."). Further, establishing new, databases of Internet traffic data with personal information that ISPs had not previously stored would create an attractive target for hackers and data thieves, and increase the risk of accidental disclosure. The result is greater risk of data breach litigation, with attendant increases in security, insurance and litigation costs.

traffic inspection and warehousing capability that would be required to meet this obligation.[294/] Thus, contrary to NRF's suggestion, there are important public policy bases for limiting the full brunt of notification obligations to breaches of subscriber data stored or maintained by an ISP – as distinct from data that may be transiting their networks.[295/]

E. Other Proposed Restrictions Are Impermissible or Counterproductive

Other proposed restrictions are not supported by the record and should not be adopted. First, the Commission should not preemptively bar any ISP data use practices, such as service discounts in exchange for consent to use customer data for advertising and marketing.[296/] As ITIF notes, the Commission's proposal to ban such arrangement is "remarkably anti-consumer."[297/] Consumers' Research observes that this proposal is antithetical to "true consumer choice," because it "presumes that all consumers have the FCC's preferences" and fails to "respect[] the many consumers who make this exchange based on their own preferences."[298/] As

---

294/ Feamster at 6 ("DPI is typically not widely deployed in many ISP networks. Several ISPs have stated in various forums that DPI capabilities are deployed on less than 10% of the link capacity in an ISP network; even if DPI were widely deployed, the cost of retaining the traffic that could be collected from DPI for any length of time would be prohibitive.").

295/ The kind of limiting language for service providers decried by NRF has long been a part of the law regulating shippers of goods and communications carriers so as to avert carriers from inspecting the contents of the materials or information they transmit. *See, e.g.*, 49 U.S. C. § 80113; 17 U.S.C. § 111(a)(3). The service provider exemption in the Digital Millennium Copyright Act is likewise designed to obviate content-based examinations of material transmitted or hosted by service providers. 17 U.S.C. § 512(a),(m).

296/ *See* NCTA at 94. According to FTC Commissioner Ohlhausen, the *Notice* "mischaracterizes the FTC's findings about what the FCC labels 'financial inducement practices.'" Contrary to the Notice, the FTC's Big Data Report claimed that some workshop participants raised concerns with this issue, but the FTC itself has never expressed such concerns. Ohlhausen at 3.

297/ ITIF at 14; *see also* T-Mobile at 44 ("Recent research strongly suggests that customers in many cases voluntarily elect to make such trade-offs, and that they benefit from the ability to do so; these studies also show that such choices are consumer- and context-specific.").

298/ Consumers' Research at 8; *see also* MMTC at 8; Verizon at 45-46; SIIA at 12-13.

the Multicultural Media, Telecom and Internet Council and others point out, these programs can drive online usage, especially among low-income consumers.[299/]

A variety of commenters agree that so long as the options and impact are clearly presented, the Commission should allow consumers to decide for themselves whether or not they are beneficial. As T-Mobile states: "Consumers should be free to decide what they care about and what they value, as long as the choices provided to them are made clear and they have other choices in the marketplace."[300/] CDT avers that "BIAS providers should still have flexibility under the rules to encourage customer opt-in, including offering monetary rewards in exchange for customer opt-in."[301/] MMTC contends that "financial inducement programs that require informed consent should not be seen as presumptively coercive, *i.e.*, consumers should have sufficient information provided to understand the benefits of such services and make their choices."[302/]

As several commenters point out, to the extent Section 222 applies to ISPs, the law in fact bars the Commission from prohibiting the practice *because* it eliminates consumer choice. "The opening clause of Section 222(c)(1) sets forth that "[e]xcept as required by law *or with the approval of the customer*," a telecommunications carrier may not engage in certain practices involving CPNI.[303/] This "make[s] clear that Congress envisioned a regime in which customers

---

299/ MMTC at 8; Ohlhausen at 3; AT&T at 59 ("Banning discounts in exchange for information-sharing would, by definition, increase the price and lower the output of any affected service, including broadband Internet access. The contemplated ban would thereby disadvantage precisely those low-income populations about whom the NPRM expresses concern.").

300/ T-Mobile at 45.

301/ CDT at 3. The specific conditions on data-related discounts proposed by CDT – particularly the requirement to disclose to the government the zip+4 location of all customers participating in such programs - are unnecessary. *See id.* at 25.

302/ MMTC at 8.

303/ CTIA at 46 (emphasis in original).

would have the option to consent to the use or disclosure of their personal information"[304/] and the Commission is not authorized to eliminate that option.

A ban on financial inducements or data-related discounts also would violate the First Amendment.[305/] As Verizon comments, "the Commission contemplates banning the offering of discounts not for any reason related to the economic impacts of those discounts, but to prevent broadband providers from persuading customers to agree to share their information."[306/] This fails the *Central Hudson* test[307/] because it restricts ISPs' speech rights and neither advances a substantial government interest nor is narrowly tailored.[308/]

Second, commenters demonstrate that the Commission lacks authority to ban or restrict arbitration clauses, which Federal policy strongly favors[309/] Commenters point out that under the Federal Arbitration Act ("FAA"), arbitration provisions are "valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract."[310/] This "applies to all arbitration agreements and to all categories of claims unless Congress overrides the FAA in another federal statute"[311/] by express means.[312/] The Communications Act does not, however, expressly grant the Commission authority to override the Federal Arbitration Act.[313/]

304/ Verizon at 47.

305/ Verizon at 50-53.

306/ Verizon at 51.

307/ *See supra* Section I.

308/ Verizon at 52.

309/ NCTA at 94, n. 348; Comcast at 102-106; ITTA at 25 *citing AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 346 (2011) (the FAA "embod[ies] [a] national policy favoring arbitration") and *Am. Exp. Co. v. Italian Colors Rest.*, 133 S. Ct. 2304, 2309 (2013); Hughes Network Systems at 8.

310/ CTIA at 55; Verizon at 72 *citing* 9 U.S.C. § 2.

311/ Comcast at 102-03; CTIA at 56 *citing Shearson/Am. Express, Inc. v. McMahon*, 482 U.S. 220, 226 (1987).

Arbitration is also pro-consumer. "[T]he flexibility, length, efficiency, likelihood of success, and lower expenses of arbitration make arbitration a much more consumer-friendly option than forcing consumers to seek redress through the already crowded court system."[314/] Consumers' Research notes that "[w]ith arbitration, consumers tend to recover greater monetary benefits—166 times greater—than in litigation."[315/]

Third, the Commission should not prophylactically restrict use of any particular data management technology, such as DPI. As NCTA wrote in its initial comments, entities other than ISPs have the access to the same or similar information as ISPs can obtain through DPI.[316/] Commenters note that edge providers review email contents and social media posts to provide relevant advertising alongside,[317/] and there is no evidence in the record to suggest that ISPs are engaged in the kind of ubiquitous collection and use of customer communications content undertaken by large edge providers. As Professor Feamster observes, "DPI is a red herring."[318/] It is not widely deployed and the cost of retaining traffic obtained through DPI is prohibitive.[319/] Further, consistent with NCTA's initial comments, Professor Feamster notes that DPI is typically

---

312/ CTIA at 56; Verizon at 74 *citing CompuCredit Corp. v. Greenwood*, 132 S. Ct. 665, 672 (2012); Comcast at 102-103 ("[A]n arbitration provision cannot be invalidated by a state law or agency rule that is aimed at discouraging the use of such a provision unless Congress explicitly permits such a rule.").

313/ Comcast at 105; CTIA at 56-59; Verizon at 74; Consumers' Research at 5-6.

314/ Comcast at 106; Hughes Network Systems at 8(Arbitration "is frequently used by broadband service providers to expedite resolution of disputes and reduce costs incurred in litigation, allowing savings to be passed directly to consumers.").

315/ Consumers' Research at 5.

316/ NCTA at 95.

317/ Verizon at 42-43; Cincinnati Bell at 9.

318/ Feamster at 6.

319/ *Id.*

used to help operators manage and secure their networks.[320/] Rather than preemptively restricting the use of some particular technology or technique like DPI, the Commission should heed the FTC's approach of ensuring that privacy frameworks are technology neutral.[321/]

Fourth, the Commission cannot restrict ISP collection and use of data from publicly available, third-party sources.[322/] Section 222(h)(1) specifies that CPNI constitutes only information "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[323/] Information about a customer obtained from a publicly available third party source is neither made available "by the customer" nor furnished "by virtue of" the relationship between carrier and customer, and therefore its acquisition or use cannot be constrained by Section 222.[324/]

IV. THE CONSENSUS PRIVACY FRAMEWORK IS THE BEST WAY TO ADAPT THE FTC PRIVACY REGIME TO BROADBAND SERVICE

In light of the host of policy and legal defects in the *Notice*, NCTA and other commenters again urge the Commission to look to the Consensus Privacy Framework to protect broadband consumer privacy, preserve a uniform set of rules for the Internet ecosystem, and enable ISPs to continue to have the same opportunity as all other online entities to provide their customers with

---

320/ Feamster at 6; NCTA at 95.

321/ NCTA at 95 *citing Protecting Consumer Privacy in an Era of Rapid Change*, FEDERAL TRADE COMMISSION, at 56 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; *see also* WTA at 24 n. 57 (citing the FTC Privacy Report as noting strong concerns about use of deep packet inspection without consent, but expressly excluding from those concerns the use of deep packet inspection "for network management, security, or other purposes consistent with the context of a consumer's interaction with their ISP.").

322/ *See* NCTA at 21-2, 83.

323/ 47 U.S.C. § 222(h)(1). Indeed, Section 222 contains no restrictions on data collection *at all*. NCTA at 89-90.

324/ NCTA at 21; CTIA at 48-49; Comcast at 75 ("Thus, it does not include any data that the carrier may obtain outside of this relationship, such as from a third party.").

the benefits of data-driven innovation.[325/] The Consensus Privacy Framework, developed by a broad cross-section of industry associations representing ISPs, technology companies and others, aligns closely with the FTC Framework that has effectively protected consumers for many years and builds on the White House's national consumer privacy blueprint, which balances the goals of providing meaningful privacy protections while promoting the continued vibrancy of the Internet marketplace.

Chairman Wheeler himself has stated that the Commission's approach should be "consistent with the kind of thoughtful, rational approach that the FTC has taken"[326/] and "firmly rooted in the privacy protection work done by the FTC."[327/] While commenters agree that the Commission's proposal fails to accomplish that objective, [328/] the Consensus Privacy Framework is expressly designed to faithfully adapt the FTC's Framework to the FCC context. As former FTC Chairman Jon Leibowitz recently testified, "an FCC rulemaking consistent with the FTC's privacy framework would ensure that privacy enforcement remains both robust and technology neutral—that is, based on the sensitivity of data collected and how that data is used, rather than on the type of entity collecting the data."[329/]

The Consensus Privacy Framework takes that approach. It is predicated upon the core privacy principles of transparency, consumer choice and respect for context, and security. It is

---

325/ NCTA at 100-103; WISPA at 8-24; Comcast at 21-23; Competitive Carriers Association at 5-10; ACA at 39-42; CTIA at 76; USTelecom at 10; *see* also Verizon at 7-15.

326/ Margaret Harding McGill, *FCC, FTC Chiefs Zero In On Data Security, Privacy,* Law360, Jan. 6, 2016, *available at* http://www.law360.com/articles/743314/fcc-ftc-chiefs-zero-in-on-data-security-privacy (quoting FCC Chairman Tom Wheeler).

327/ Testimony of Tom Wheeler, Chairman, Federal Communications Commission, before the Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law (May 11, 2016).

328/ *See supra* Section II.A.

329/ Testimony of Jon Leibowitz, before the House Energy & Commerce Committee, Subcommittee on Communications and Technology (June 14, 2016).

grounded in providing consumers with consistent and predictable privacy protections and prohibiting unfair and deceptive industry privacy practices. Further, the Consensus Privacy Framework is designed to give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI. As ACA notes: "A flexible 'unfair and deceptive' approach as outlined in the Industry Proposal would meet consumers' privacy needs while allowing them to take advantage of innovative products and services, and would avoid inconsistent oversight."[330/] The benefits of the Consensus Privacy Framework also "resonate more clearly for small broadband providers, which will under the Industry Framework be able to retain existing privacy policies that are compliant with FTC policies, state law requirements and longstanding industry practices."[331/]

The Consensus Privacy Framework would preserve a consistent policy across the Internet for uses and disclosures of broadband customer data in accordance with the existing FTC Framework. This approach will avoid consumer confusion and establish a more flexible and less burdensome set of rules that will strengthen competition, promote innovation, and ensure that ISPs have the same opportunity to provide data-driven services to their customers as all other Internet companies.[332/]

330/ ACA at 42; WISPA at 11 (Adopting this Framework "will allow a seamless transition between the [FTC and FCC], reduce administrative burdens, avoid duplication of regulations and provide certainty for providers and their customers, with appropriate enforcement mechanisms.").

331/ WISPA at 10.

332/ Competitive Carriers Association at 7; CALinnovates at 5; CTA at 11-13; Consumers' Research at 11-12; ITIF at 10-12; ITI at 9-10.

CONCLUSION

For the reasons set forth here and in NCTA's initial comments, the Commission should refrain from adopting the rules proposed in the *Notice* and instead adopt an approach similar to the Consensus Privacy Framework.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta Polk
Jennifer K. McKee
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431

William A. Check, Ph. D
Senior Vice President
Matthew Tooley
Vice President of Broadband Technology
Science & Technology

Christopher J. Harvie
Ari Z. Moskowitz
Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.
701 Pennsylvania Avenue, N.W.
Suite 900
Washington, D.C. 20004-2608

July 6, 2016